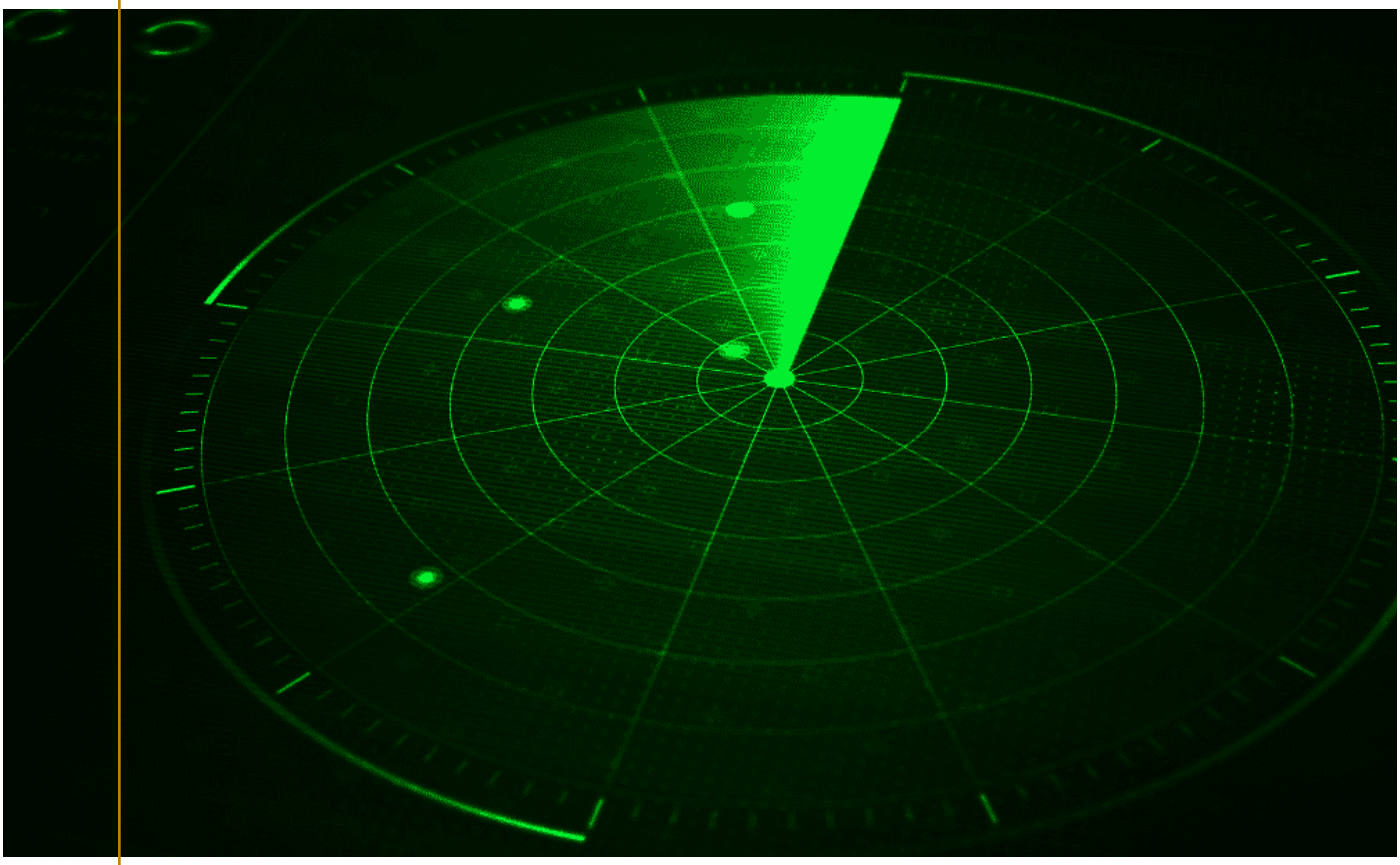
Australian National University | NATIONAL SECURITY COLLEGE

Maritime Domain Awareness 3.0

The future of information and intelligence-sharing in the Indian Ocean

David Brewster | Simon Bateman

REPORT SEPTEMBER 2024



The authors

David Brewster

Dr David Brewster is a Senior Research Fellow with the National Security College. He is one of Australia's leading experts on maritime security in South Asia and the Indian Ocean region. He advises government agencies in Australia and around the Indian Ocean on maritime security issues, including maritime domain awareness and environmental security.

Dr Brewster's books include India as an *Asia-Pacific power*, about India's strategic role in the Asia-Pacific, *India's ocean: the story of India's bid for regional leadership*, which examines India's strategic ambitions in the Indian Ocean, and *India and China at sea: competition for naval dominance in the Indian Ocean*.

Dr Brewster, together with Simon Bateman and Anthony Bergin, are authors of the recent report, *Governing Bangladesh's maritime space: An assessment of Bangladesh's maritime challenges and maritime domain awareness capabilities*.

Simon Bateman

Captain Simon Bateman retired from full-time service in the Royal Australian Navy in 2021 after serving for nearly 40 years in various aviation and seagoing roles. His last position in the Navy was as the Australian Defence Adviser in New Delhi, India.

Captain Bateman is an alumnus of the Indian National Defence College, New Delhi, where he completed his studies in 2017. He also holds a Master of Maritime Studies from the University of Wollongong and a Master of Management (Defence Studies) from the University of Canberra.

Acknowledgements

This report builds on work undertaken by the NSC with support from the Australian Department of Foreign Affairs and Trade, in facilitating discussions among MDA practitioners on the enhancement of regional information-sharing arrangements in the Indian Ocean. The authors would like to acknowledge the helpful comments and suggestions on this report from Dr Anthony Bergin, Senior Fellow at Strategic Analysis Australia and expert associate at the; Mr Peter Ford, Senior Advisor at the NSC; Mr Ben Scott, Senior Adviser at the NSC, Mr Greg Clifford of CRIMARIO II; Professor Christian Bueger of the University of Copenhagen; Dr Jeffrey Payne of the Near East South Asia Center at the National Defense University, Washington DC; Dr Jane Chan of S. Rajaratnam School of International Studies at Nanyang Technical University, Singapore; Mr Brett Peppler of Intelligent Futures; and relevant Australian agencies. We also thank Dr Jane Chan for coining the term 'Maritime Domain Awareness 3.0'. All opinions expressed in this report are the authors' alone.

ANU National Security College
national.security.college@anu.edu.au

The Australian National University Canberra ACT 2600 Australia
www.anu.edu.au

CRICOS Provider No. 00120C
TEQSA Provider ID: PRV12002 (Australian University)

Cover illustration: Marineinsight.com

Contents

Executive Summary and key findings

- ***MDA systems being disrupted by new information rich environment:*** Maritime domain awareness (MDA) systems around the Indian Ocean region are being disrupted by technological developments, including a proliferation of satellite sensing and new analytical tools. This has significant implications for MDA information-sharing arrangements in the Indian Ocean and beyond.

Implications for MDA users

- ***Greater use of open-source information:*** MDA users such as maritime enforcement authorities are now gaining much greater access to information from a wide range of diverse sources, and this trend is likely to increase significantly in future. This includes much greater use of open-source information, including from private companies and NGOs. The long-standing monopoly that government agencies have had in MDA is being challenged.
- ***Greater reliance on analytical tools:*** The growing availability of online analytical tools using image recognition and machine learning technologies can help to process large volumes of data to make it useful for further analysis and operational purposes. The volume of data will still likely place significant strain on the analytical capabilities of Indian Ocean countries, which are already thin.
- ***Democratisation of information and intelligence:*** The proliferation of alternative information-sharing systems may effectively democratise maritime information and intelligence in several ways. Smaller or less wealthy countries may become considerably less reliant on larger countries for information.
- ***Greater pressure on response capabilities:*** These developments may make broad swathes of the ocean observed from spaces for the first time. This will place greater pressure on countries to have adequate response capabilities, potentially requiring enhanced cooperation arrangements with other countries.

Implications for Australia

- ***Building national capabilities of selected Indian Ocean partners:*** Australia's policy is to help Indian Ocean partner states build sovereign national maritime security capabilities, including MDA capabilities, to enhance governance of their national jurisdictions and beyond. But there are significant constraints on resources that it can commit to capability building the Indian Ocean region. This means that Australia should leverage its strengths such as its expertise in MDA systems.
- ***Help build common information-sharing platforms:*** Australia should work with Quad and other like-minded partners to further develop the US-sponsored *SeaVision* system or establish a new common information platform where MDA users can select from a menu of information products offered by governments and non-governmental sources. The principal objective should be to establish a common information platform that is used around the region, rather than creating a universal common operating picture.

- ***Opportunities to take the lead in niche areas:*** Australia could consider taking a leading role in niche MDA areas involving the development of information and response networks with selected Indian Ocean partners. This could include using existing specialist Australian agencies/capabilities in the following areas:
    - Cyber
    - Cable resilience
    - Environmental protection.
- ***Help build analytical capabilities:*** Australia could also make a valuable contribution in using its expertise to help selected Indian Ocean partners build their MDA analytical capabilities (which is likely to come under ever greater stress).

Consequences for regional information-sharing centres

- ***Need to adapt:*** Regional information-sharing centres (ISCs) will need to adapt to these developments to ensure that they remain relevant mechanisms for regional cooperation. In many cases, they may find it difficult to compete directly with online platforms as sources of tactical or operational intelligence for MDA users around the region.
- ***Review information-sharing systems:*** The reliance of regional ISCs on communication through International Liaison Officers does not provide an optimal solution for national MDA users seeking real-time or near real-time operational information and intelligence.
- ***Providers of strategic intelligence:*** Regional ISCs may need to more clearly define what they do and don't do. They could remain a valuable source of strategic intelligence/trend analysis, that is, as a source of historical information that can be used in tracking and understanding broad trends in regional threats.
- ***Improve use of International Liaison Officers:*** International Liaison Officers appear to be under-utilised as conduits for information-sharing. Their presence at regional ISCs is a potentially highly valuable resource and their roles could be expanded more towards regional liaison and multilateral response coordination and other roles.

Organising for a new information rich environment

- ***Challenge of integrating open-source:*** The growth of a new information-rich environment will involve the diversification of information sources, requiring improved integration of open-source information with non open-source information.
- ***Importance of human intelligence:*** There will be no single answer to the challenge of establishing effective MDA, and despite technological developments, MDA users will still need to access information of many different types. For example, the ease of information provided through new platforms should not be allowed to obscure the importance of human intelligence, which can be crucial in understanding the behaviour of maritime actors, and may not be replicated by technology.
- ***Need for common information platforms:*** There is a need for a platform that can help users effectively aggregate, correlate and analyse different sources of data that they individually wish to access. This should facilitate commercial and NGO entities to 'plug and play' their products in a common platform where MDA users can select from a menu of products provided by governments, companies and NGOs, according to their circumstances. Given that users may choose to access different information sources, this would not necessarily create a universal common operating picture.
- ***New common information platform.*** The architecture of the US-sponsored *SeaVision* platform may be a source of sensitivities among many MDA users in Indian Ocean states, and these sensitivities will likely become increasingly apparent. The Quad partners should consider creating a new common platform that is perceived to be more multilateral and transparent in nature than existing offerings.
- ***Involving public and private agencies:*** The management of such a common information platform by a consortium of civilian agencies and, perhaps, private companies, would also go some way towards mitigating political/geostrategic anxieties held by some MDA user countries. The involvement of private companies in such a platform may also be a way of mitigating costs.

Introduction

For many years, Australia largely neglected its 'Second Sea'. However, it is now giving ever greater attention to the Indian Ocean as part of a determination to make an active contribution to the regional strategic balance.[1]

Australia's approach to the Indian Ocean emphasises the sovereign aspirations of countries in the region. Foreign Minister Penny Wong recently described Australia's vision for: "A region that is peaceful and predictable, that is governed by accepted rules and norms, where all of us can cooperate, trade and thrive. Where a larger country does not determine the fate of a smaller country. Where each country can pursue its own aspirations. Where no country dominates, and no country is dominated."[2]

Those principles underlie Australia's current contribution to regional security by helping to build the sovereign national capabilities of its Indian Ocean partners.

For many years, the Indian Ocean was the 'wild west' of the world's oceans, a space where numerous maritime security threats affected some of the world's most important trading lanes and the prosperity and stability of many countries. These challenges underline the need for Australia and its partners to support regional maritime security.

Australia's efforts to help develop the capabilities of Indian Ocean partners include bolstering their ability to uphold international norms and respond to a range of maritime threats. Importantly, it also involves enhancing their maritime domain awareness (i.e. their situational awareness in the maritime domain) as an essential foundation for their ability to govern their maritime jurisdictions.

Building effective MDA requires effective monitoring and surveillance capabilities and effective mechanisms for sharing of information and intelligence. These have now become an important focus for regional maritime security.

However, technological developments are now disrupting traditional approaches to building MDA. In particular, the proliferation of satellite-based sensing and computer analytics is creating a new information-rich environment. This will have significant consequences for regional cooperation in the Indian Ocean.

This report is divided into five sections:

Section One discusses why MDA is an essential prerequisite to enhancing maritime security in the Indian Ocean, and then explains the ways in which effective MDA can be achieved.

Section Two describes the current state of MDA architecture in the Indian Ocean, including the development of national fusion centres and then the establishment of regional information-sharing centres to promote the sharing of information between different countries.

Section Three discusses the evolution of a new information-rich environment, including the proliferation of earth observation satellites with new types of sensors and the availability of automated analytical tools, and how this is creating a virtual deluge of information and intelligence for MDA users.

Section Four discusses the development of new web-based information-sharing platforms being offered by governments, private companies and NGOs. Collectively, these give MDA users many new options to access information.

Finally, Section Five assesses the implications of these developments for MDA users, for regional information-sharing systems and for Australia. It concludes that Australia and its like-minded partners can play an important role in facilitating Indian Ocean countries building effective MDA and maritime security capabilities within this new information rich environment.

We hope that this report will be a useful basis for further discussions about these issues by MDA practitioners and policy-makers around the region. A glossary of terms used in this report is contained in Appendix 1.

David Brewster

Simon Bateman

Canberra

September 2024

Section 1: Imperatives to share maritime information and intelligence

This section looks at why many Indian Ocean states are giving priority to MDA as an essential foundation for maritime security. It considers how MDA is developed, the imperatives to share maritime information and intelligence, as well as some of the political or strategic aspects of MDA.

Why is there a focus on enhancing maritime domain awareness in the Indian Ocean?

The Indian Ocean is the 'wild west' of the world's oceans. It is a maritime space where multiple maritime security threats and challenges have the potential to affect regional security and stability and interfere with some of the world's most important trading lanes.

The Indian Ocean, particularly in the northwest region, faces many conventional naval threats from actors such as Iran and its proxies such as the Houthi insurgents. China's growing naval presence is also creating anxieties for many countries. But in many parts of the Indian Ocean, maritime threats are often principally transnational in nature, including piracy, drug smuggling, people smuggling, illegal fishing and shipping accidents, in addition to the impacts of climate change and other environmental threats.

For many Indian Ocean countries, these transnational threats represent a major security priority.[3] Among other things, these threats can have a significant impact on the ability of Indian Ocean states to exploit marine resources and protect the vital trade and communications on which they depend for economic development and prosperity.

Many of these maritime threats go largely unaddressed by either local or extra-regional countries. This reflects the number and variety of challenges, the lack of maritime surveillance and response capabilities of many states, and the huge size of the ocean. Indeed, many Indian Ocean countries have little real knowledge of what is occurring in their own maritime jurisdictions, let alone in the expanse of high seas beyond, and are unlikely to have adequate capabilities to respond to all threats.

Consequently, many Indian Ocean states are increasingly giving high priority to enhancing their MDA to improve their situational awareness in the maritime domain — knowing what is occurring on, above and below the water — as an essential starting point to enhancing maritime security. Without such an understanding, there is little chance for regional states to properly govern and respond to threats in their maritime spaces.

Given the huge size of the Indian Ocean, it is not feasible to have complete real-time situational awareness over the entire ocean space. Achieving 'effective' MDA means achieving a degree of situational awareness over a selected maritime space sufficient for relevant authorities to understand and potentially respond to a particular maritime threat. Achieving *effective* MDA may involve quite different considerations and geographic spaces, depending on what the identified threat is. Effective MDA will differ according to whether the identified threat is, say, illegal fishing or people smuggling or potential shipping accidents. In other words, effective MDA is not a singular or permanent state of affairs.

Most countries focus on trying to achieve limited situational awareness in their immediate waters, including their territorial seas and exclusive economic zones, although countries such as Australia also try to 'see' as far beyond that as possible to gain longer notice of approaching threats.

How do you build effective maritime domain awareness?[4]

Building effective MDA can be difficult in practice. It involves a lot more than sending an aircraft out to spot, say, an illegal fisherman or a drug smuggler. The ocean is huge, and usually too big to find things without having a good idea of where to look first. This often means compiling large amounts of data from different sources and making sense of it to identify vessels of interest that require further investigation.

Building maritime domain awareness typically involves pulling together information on the maritime domain that was created for different purposes by a wide range of sources. This includes information from Automatic Identification Systems (AIS), Long Range Identification and Tracking systems, Vessel Monitoring Systems, regional and national vessel registries, customs and port intelligence, criminal investigations, data from coastal radar, aircraft (crewed and uncrewed), satellite, ocean surface and undersea sensors, and information from ocean users such as shipping companies, fishers, coast watchers, and more.

Many countries in the Indian Ocean region have established national information fusion centres to help improve MDA for government agencies such as navies, coast guards and fisheries agencies that have responsibilities in the maritime domain. These national fusion centres correlate or 'fuse' data from many different sources to produce a 'common operating picture'. In broad terms, this is a consolidated picture of vessels or other developments in each maritime space, based on all available information.

There are significant challenges in creating a common operating picture using data from such a wide range of different sources, of differing quality and trustworthiness, and including both classified and open-source information. One of the biggest challenges in creating a common operating picture is the civil-military-commercial divide. Data on the maritime domain is sourced from a variety of military, law enforcement and civil government agencies, as well as commercial entities. Each will have its own agenda, laws, motivations and concerns about information security based on national security considerations or commercial sensitivities. Military agencies will be wary of sharing information of a military nature. For private bodies, the location, course, speed and cargo of a particular ship, or the favoured fishing grounds of fishing vessels, can be significant commercial secrets that would be of great interest to competitors.

AIS data often provides a starting point in creating a common operating picture, particularly in determining the location of commercial vessels. AIS devices are automatic transmitting devices required to be operated by larger transport vessels under International Maritime Organization (IMO) rules,[5] which transmits a vessel's location and other information about the vessel. The IMO requirement to transmit AIS data is supplemented by rules of some countries, many countries do not effectively enforce it. AIS transmissions were originally only gathered by terrestrial receivers and other ships, but since 2008 also they also transmit to satellites. AIS data is open-source information available online. Figure 1 shows a screenshot of AIS data on commercial vessels in the northern Indian Ocean and Southeast Asia.

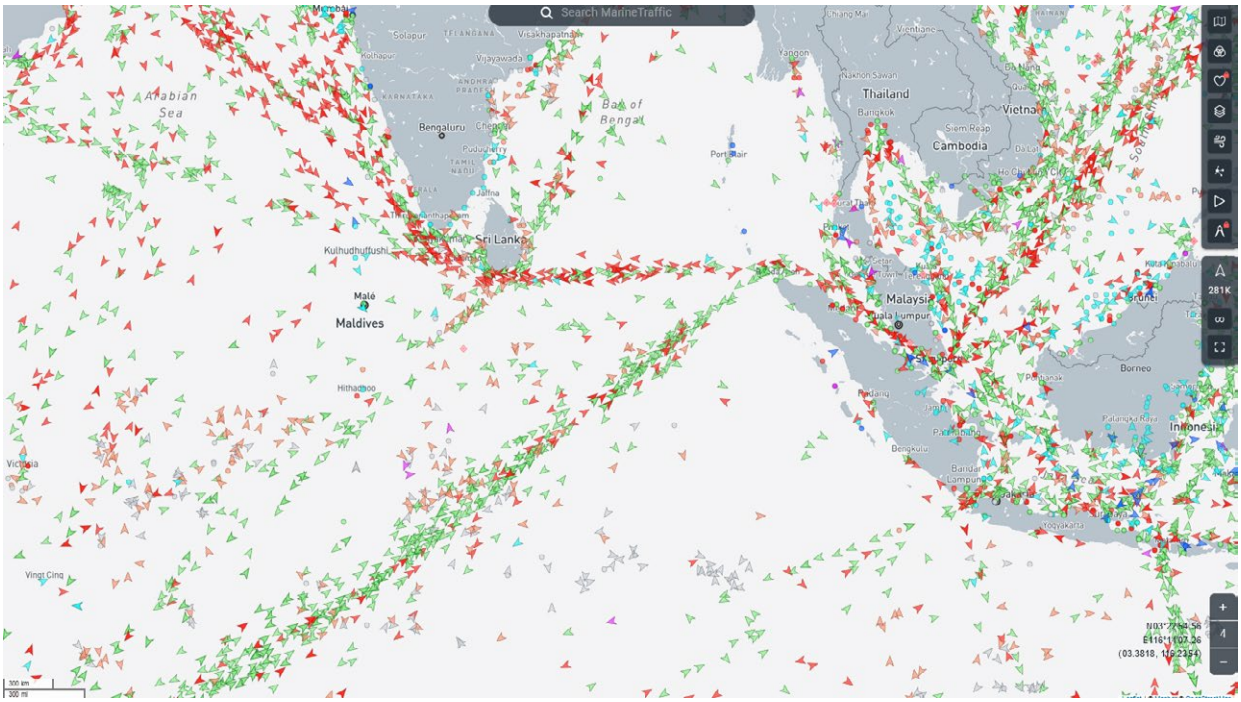


Figure 1: Screenshot of AIS data on vessels in the northern Indian Ocean as at 11.35am on 11 July 2024. (Source: Marinetraffic.com)

But while AIS data are extremely useful, AIS only provides data on vessels that *want* to be seen. Despite IMO rules, many vessels do not carry AIS devices or other automatic location devices. If they are carrying an AIS device, they may switch it off so go 'dark' and cannot be seen, or 'spoof' their AIS devices (i.e. interfere with the devices so that they transmit false vessel identities or locations). Indeed, there are a whole range of practices that allow vessels conducting illegal activities to hide in plain sight, such as 'laundering' vessel identities by swapping identities with 'clean' vessels or 'zombie' vessels that have been scrapped.[6] The identification of vessels that have their AIS devices switched off is an important step in identifying potential bad actors, but in some cases the behaviour of vessels that are apparently transmitting by AIS may also need to be investigated. This is why it is necessary to use data from multiple sources, particularly to determine vessels that may be involved in unlawful activities.

Another type of automatic identification devices is a Vessel Monitoring Systems (VMS). These are widely used in the monitoring of fishing fleets. Like AIS devices, these automatically transmit a vessel's location to satellite or terrestrial receivers. However, unlike AIS, VMS devices are fitted to fishing vessels and their data is generally available only to national fisheries agencies. While VMS are principally used for fisheries management, the data can have significant value in countering piracy, or the use of fishing boats for purposes such as drug running or people smuggling.[7] However, there may be commercial sensitivities about sharing such data with other countries, and there may be concerns about illicit fishing by neighbours. Some Indian Ocean countries are prepared to share VMS data with others, but others may be quite reluctant to do so, significantly limiting the value of VMS data as a regional MDA tool.

The other key position-reporting tool is the Long Range Identification and Tracking (LRIT) system. LRIT regulations apply to all passenger ships, cargo ships larger than 300 tonnes, and mobile offshore drilling units. A vessel's flag state will generally require a ship report its position every six hours. However, like AIS, the system can be manipulated to not report, provide wrong position data or transmit an incorrect maritime mobile service identity (MMSI).

Systems such as AIS, VMS and LRIT are all essentially self-reporting tools that historically have been supplemented from data gathered from many other sources, including, for example, from maritime aerial surveillance and shipping and fishing industry sources. Notably, effective MDA often requires inputs from people who have an understanding of the patterns of life of maritime actors.

In recent times it has become increasingly possible to correlate AIS, VMS and LRIT data with data coming from various satellite earth observation systems, particularly those commonly found in low earth orbits. This helps identify vessels that are not transmitting their positions for whatever reasons. These satellites can now provide a range of data on surface and even subsurface activities from several different types of sensors. In broad terms, these include the following:[8]

- Electro-optical (EO) imagery that can produce imagery of a wide area (or, with appropriate cueing, on selected vessels). EO derives data from the ultraviolet through the infrared portions of the electromagnetic spectrum. EO sensors are typically passive, which means they use natural electromagnetic energy sources such as the sun, naturally occurring radiation, or emitted heat. They generate data by capturing the reflected or emitted electromagnetic energy from an object. These sensors, which operate only in a passive or 'receive' mode, do not emit energy. The effectiveness of electro-optical sensors can be degraded or denied by adverse weather, light conditions, and atmospherics.
- Visible Infrared Imaging Radiometer Suite (VIIRS), used to detect light emissions from vessels.
- Synthetic Aperture Radar (SAR) is a type of radar that can detect vessels or other objects. SAR detection can be used at night or through clouds. SAR illuminates objects with pulses of microwave energy. It is generally used over a wide area, but if commanded by the satellite operator, the radar can be refocused to produce high-resolution images of a single vessel; and
- Radio Frequency (RF) detection, involving the detection of the location of vessels through radar or radio emissions.

Data from earth observation satellites can be extremely useful in locating and identifying potential vessels of interest, including through tracking their behaviour. But this data can also be used for many other purposes in improving situational awareness in the maritime domain. For example, satellite data (including EO imagery and SAR) can be used to detect oil spills and other environmental developments.[9]

In future, data from earth observation satellites will likely be supplemented by considerable amounts of data from a range of new surface and subsurface sensors (including from surface drones, wave gliders and fixed-cable sensors). This will be discussed in greater detail in section three of this report.

But collecting data from many sources is not enough. Data from different sources needs to be correlated or fused, and then analysed or made sense of to turn it into awareness or intelligence. For these purposes, we define 'intelligence' as information that has been analysed and refined so that it is useful to policymakers in making decisions.[10] Intelligence can be used for military or non-military purposes, and in the case of MDA it is principally used in support of maritime law enforcement efforts. Producing maritime intelligence traditionally required human analysts with a deep understanding of marine affairs and shipping and fishing industries, but there is an increasing reliance on automated analytical tools to process large amounts of data.

The maritime intelligence product can be of different types. Maritime intelligence may be *operational or actionable intelligence* about a particular threat, that may, for example, include the location, heading, speed of a vessel of interest, who is operating it, and what it may be doing or intending to do. Operational intelligence about a particular vessel can then provide a basis for decisions about an appropriate response by relevant maritime law enforcement agencies to a particular threat.

Maritime intelligence can also be *strategic intelligence* about the overall threat picture, including the trajectory of newly emerging threats. Strategic intelligence analysis is intended to provide longer-term assessments on emerging threats, which reduce uncertainty while also providing warning for senior decision-makers.[11] Strategic intelligence is essential for maritime enforcement authorities to establish priorities, allocate resources and, potentially, pre-empt future threats.

One of the biggest problems in building maritime domain awareness comes from the vast size of maritime spaces and the transnational character of the maritime industries, where for instance a single transport vessel might involve dozens of different jurisdictions (e.g. flag state, owners, charterers, crew, cargo ownership, origin and destination). Achieving even limited situational awareness in the maritime domain is usually beyond the resources of many countries, acting alone. For nearly every country in the world, it is only possible to build MDA through the mutual sharing of maritime information and intelligence with other countries and stakeholders.

However, cross-border information-sharing by countries involves further complications. There are heightened concerns about maintaining security of classified information, and national agencies may be concerned about maintaining commercial confidentiality in relation to that country's merchant or fishing vessels. Some agencies may, for example, acquire shipping information from commercial providers on terms that it cannot share with other countries. Law enforcement authorities may be unwilling to share information with other countries due to potential consequences for citizens, or are restricted by privacy and other national laws. Complications such as these that might potentially be resolvable in dealing with a trusted partner can be magnified almost exponentially when contemplating sharing information on a multilateral basis.

But the fact remains that effective security in the maritime domain is frequently a collective endeavour involving more than one country. Indeed, countries can only hope to achieve security in the maritime domain through cooperation, including through sharing information and intelligence and, where possible, coordinating responses to threats. This is particularly the case in the Indian Ocean, where most states have severe limitations on the resources they can devote to maritime security.

Finally, while the sharing of maritime information and intelligence involves many technical issues, MDA cooperation, even if only for maritime law enforcement purposes, has a significant political and strategic element. Several questions might arise: Who are the partners one is prepared to share information with? How can MDA systems be used to counter or deter state-based threats? How can MDA cooperation be used to extend the power and influence of a country's decisions in the maritime domain?

These issues will be inherent not only in the information/intelligence being shared, but also in the design of MDA information-sharing systems. For example, to what extent can certain systems be used to restrict or bias flows of information to MDA users? Alternatively, to what extent can they help diversify sources of information and analysis available to MDA users?

There are concerns among some Southeast Asian countries that certain MDA systems (and even the term 'maritime domain awareness' itself) is being used by the United States as a tool to contain China.[12] China's *Global Times* has argued that the Quad's Indo-Pacific Maritime Domain Awareness Initiative, in helping Southeast Asian countries track Chinese vessels in the South China Sea, is spreading the 'Chinese threat theory.'[13] These anxieties and claims need to be acknowledged from the outset and considered in designing information- and intelligence-sharing systems that mitigate concerns and meet the needs of MDA users.

Section 2: The current state of regional MDA architecture in the Indian Ocean

This section considers the current state of regional MDA architecture in the Indian Ocean. How have Indian Ocean countries and other key stakeholders organised themselves to build MDA through their own efforts and through sharing maritime information and intelligence?

National MDA systems

The starting point for understanding MDA in the Indian Ocean and elsewhere is the role of national information fusion systems. National information fusion centres have a principal role in collecting information from domestic and international sources, creating a common operating picture, and providing intelligence to decision-makers who then decide on and coordinate an appropriate response by national maritime security agencies.

In the 20th century, building MDA was essentially the job of navies, largely relying on data provided by naval sources. This was then used to coordinate responses to threats by navy (or, perhaps, coast guard) assets. This was usually done through maritime operations centres (or 'MOCs'), which coordinated naval responses to military threats or constabulary tasks such as countering piracy or conducting search and rescue operations.

But since the beginning of this century there has been a recognition that countries need to move beyond this navy-centric approach to counter a broad range of civil maritime threats. This required access to a wider range of information than was previously the case and the coordination of multiple military and civil agencies that have responsibilities in the maritime domain.

Over the past 20 years, more and more countries have established multi-agency centres focused on civil maritime security threats, with dedicated staff that collect, fuse and analyse data and help coordinate responses. These centres are generally separate from naval MOCs, which generally operate at a higher level of security, with a principal focus on conventional state-based naval threats.

For Australia, the 911 terrorist attacks and a surge in illegal immigration by sea led to a realisation that a whole-of-government approach was required in relation to civil maritime threats. All government agencies, military and civil, with responsibilities in the maritime space were required to share information to create a single operating picture and then cooperate in a joint response to threats. The Border Protection Command[14] was established in 2005 to lead and coordinate Australian maritime security operations by military and civil agencies through a centralised operations centre, now known as the Australian Border Operations Centre (ABOC). ABOC acts as Australia's national information fusion centre for all civil maritime threats. Information is sourced not only from government agencies, but from many other stakeholders such as shipping companies and international partners. As will be discussed later, this increasingly includes information and intelligence from commercial sources and NGOs, often open source or semi-open source in nature.

Figure 2: Australian Border Force Commissioner Michael Outram at the Australian Border Operations Centre (Source: *The Australian*)

The establishment of ABOC represented a major step up for Australia's MDA, particularly in northern and Indian Ocean waters, which had a significant focus on people smuggling and illegal fishing. The work of ABOC, together with other government policies, significantly mitigated these threats to Australia's interests. These systems are never perfect, but they are quite effective as a deterrent in policing exclusive economic zones (EEZs) against many threats.

Over the past couple of decades, many other Indian Ocean countries have also established national information fusion centres, generally operated by national navies or coast guards, that fuse information from a variety of sources.

For some years, India has been moving towards a whole-of-government approach in MDA. Following the 2008 terrorist attacks in Mumbai, the Indian Navy established the Information Management and Analysis Centre (IMAC) near Delhi as India's nodal agency for maritime information and monitoring. This is currently in the process of being upgraded into a National Maritime Domain Awareness Centre that will house representatives from 15 agencies under seven government ministries.[15]

Many other Indian Ocean states have established national information fusion centres, including Singapore (Maritime Crisis Centre, established in 2011);[16] Indonesia (Sea Security Coordination Centre, established in 2014);[17] Thailand (Maritime Enforcement Command Centre, established in 2019); Pakistan (Joint Maritime Information Coordination Center, established in 2013);[18] Sri Lanka (Information Fusion Centre, established in 2022);[19] Maldives (Information Fusion Centre, due to be officially opened in 2024); and Bangladesh (Information Fusion Centre, in the process of being established).[20] Several states in the Western Indian Ocean have also established, or are in the process of establishing, national information fusion centres.

To a greater or lesser extent, these centres theoretically seek to facilitate a more whole-of-government approach to MDA, even if in practice information often remains siloed among different government agencies including fisheries, shipping and police agencies. Many countries in the Indian Ocean region also face significant resource constraints, meaning there may be very limited on-water and aerial surveillance capabilities.

In building a common operating picture of surface vessels, national fusion centres tend to rely heavily on AIS data, (their own) national VMS tracking systems installed on commercial fishing vessels, and data from platforms such as *SeaVision* and *IORIS*, discussed below. One significant challenge is the identification of vessels engaged in illegal fishing (both foreign and domestic), as well as vessels engaged in drug and human smuggling. In many cases, these vessels may go 'dark' by not transmitting or otherwise 'spoofing' their AIS or VMS data. In addition, as noted previously there are also many types of vessels that are not required to carry vessel-tracking devices. For example, Indian Ocean countries such as India, Bangladesh and Sri Lanka have large fleets of many thousands of small artisanal fishing vessels that are not required to carry tracking devices, which create significant problems for law enforcement and safety.

Regional Information Sharing Centres

While the establishment of national information fusion centres has been a big step forward in building MDA, they have their limitations. National maritime enforcement agencies may not have access to all information on activities in their areas of interest and want to be warned of threats approaching their waters at the earliest possible stage. This means they will often require information and intelligence shared by foreign partners.

While some bilateral information-sharing arrangements exist between Indian Ocean neighbours,[21] these tend to be limited in nature and may not capture information held by third parties. Consequently, 'regional' information sharing centres (ISCs) have been established to pull together and share information from neighbouring countries and other partners. These are intended to act as regional clearing houses of maritime information among participating member states. The idea is that if a whole-of-government approach to MDA is good, then a whole-of-region approach in which nations can share information and even intelligence with each other must be even better. While the ISCs principally involve sharing of information, they also distribute trend analysis that could be broadly considered a form of strategic intelligence.

In the Indian Ocean, regional information-sharing centres have been established in Singapore, Delhi, Madagascar and several in and around the Persian Gulf. In 2009, Singapore was the first to create a regional information sharing centre (Singapore IFC). In 2016, the Regional Maritime Information Sharing Centre (RMIFC) was established in Madagascar. The Areas of Interest in the Indian Ocean of the Singapore IFC and RMIFC are shown in Figure 3. In 2018, India opened the Information Fusion Centre-Indian Ocean Region (IFC-IOR), whose area of interest covers the entire Indian Ocean and beyond, into Southeast Asia and Gulf of Guinea off West Africa.

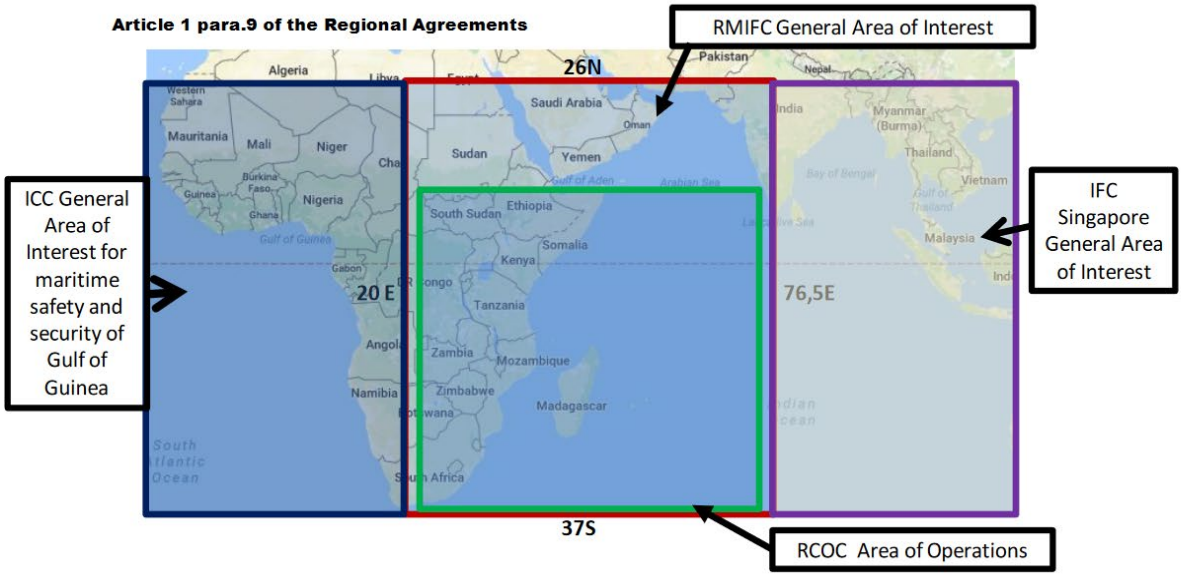


Figure 3. Areas of interest in the Indian Ocean of Singapore IFC and RMIFC. (Source: Indian Ocean Commission)

The three regional fusion centres follow broadly similar models for information-sharing. This involves channelling information to and from the regional centre through International Liaison Officers (ILOs), generally mid-ranking naval officers from partner countries that are posted to the premises of the regional centre. The ILOs are supposed to be responsible for sharing information to and from their own countries. Today, the Singapore IFC has some 26 ILOs representing 21 countries, and Madagascar RMIFC has some seven ILOs, while the Indian IFC-IOR currently has some 14-15 ILOs, with plans to build new facilities that may accommodate up to 40 ILOs.

Information is shared with regional centres through bilateral agreements between the centre's sponsor and partner countries. For example, India's IFC-IOR's information sharing operations are supported by more than 25 bilateral 'white shipping' agreements with participating countries and organisations. These are intended to facilitate the sharing of information on commercial shipping, such as data on participating countries' flagged vessels obtained through LRIT systems, but do not provide for sharing of information on so-called 'grey' or naval vessels. Nor do they provide for the sharing of national VMS data on fishing vessels or the activities of research vessels.

There are some important differences between the regional centres that could affect their relationships with participating partners. The Singapore IFC is sponsored by Singapore, which seeks to position itself as a useful information hub for the much larger Southeast Asian states around it. The Delhi IFC-IOR is sponsored by India, which seeks to position itself as the leading Indian Ocean state and as 'net regional security provider' or 'first responder' throughout the Indian Ocean.

In contrast, the Madagascar RMIFC was established pursuant to a regional multilateral arrangement among seven smaller Western Indian Ocean countries.[22] The Madagascar RMIFC is complemented by its sister entity, the Regional Coordination Operations Centre (RCOC), located in Seychelles, which is part of the same multilateral arrangement. The RCOC's role is to coordinate responses using the maritime enforcement assets of the member states and international partners. This includes some 20 naval assets and four aircraft made available by the seven partner countries, as well as regional naval and air assets of EUNAVFOR and the United Kingdom. The pooling of assets for operations that cross the maritime jurisdictions of multiple partner countries is underpinned by legal frameworks among the partners for coordinated actions at sea.

The RCOC states that it conducted some 17 combined operations between November 2020 and May 2024. As one example, Operation Yellowfin in November 2022 involved patrol vessels and aircraft from Seychelles and Mauritius interdicting an illegal fishing vessel that was almost certainly intentionally operating on the border of the Seychelles and Mauritius EEZs — which would otherwise significantly complicate the enforcement efforts by any single country (see Figure 4). The experience of the RCOC is an important reminder of the need to match regional information-sharing arrangements with regional response arrangements.

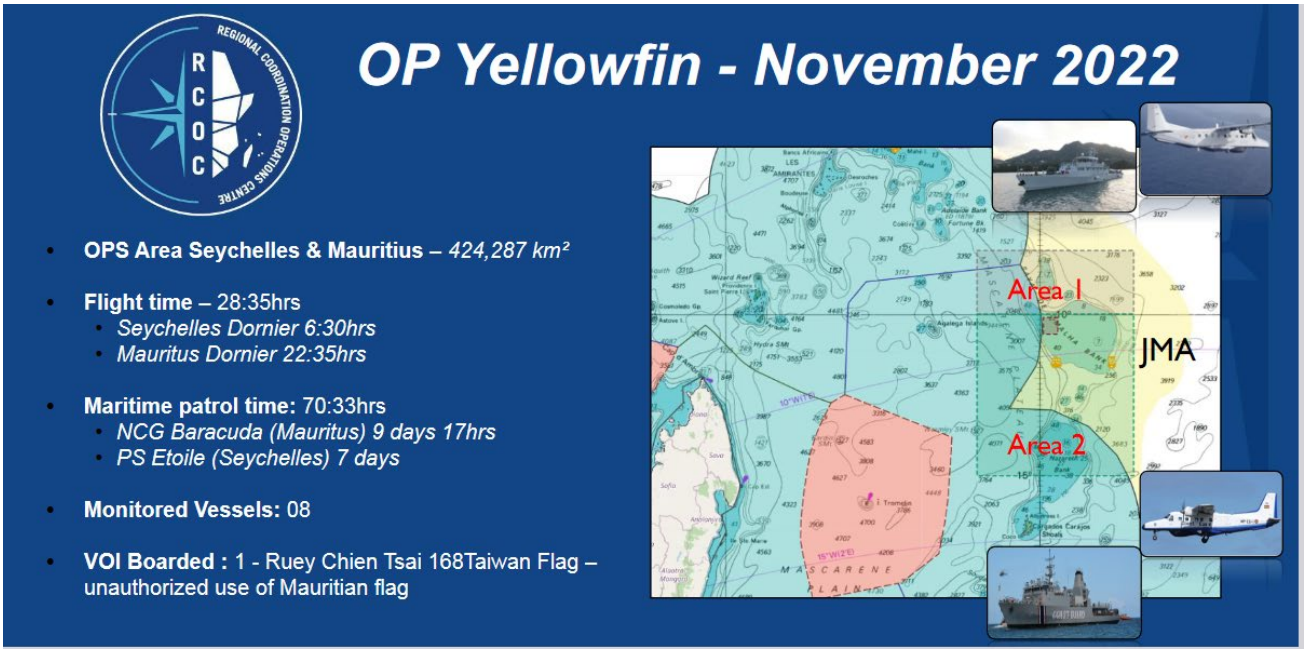


Figure 4: RCOC Operation Yellowfin (Source: Regional Coordination Operations Centre)

There are no formal institutional arrangements for information-sharing among the regional centres on an ongoing basis, other than an MoU between the Indian IFC-IOR and the RCOC. As will be discussed later, initiatives such as 'SHARE.IT' (an information-sharing tool offered by the CRIMARIO II organisation) could help in strengthening the informal exchange of data and collaboration between various information-sharing centres.

Although they deal only with non-military maritime security threats, the effectiveness of regional information-sharing centres is nevertheless constrained by geopolitical competition and national interests. The Madagascar RMIFC (and its partner Seychelles RCOC) appear to be effective in channelling and acting upon information provided by partner countries, perhaps reflecting its multilateral nature, rather than being sponsored by any single country. For the Singapore IFC, the presence of a Chinese ILO may constrain the willingness of several partner countries to share any sensitive information, while the Indian IFC-IOR's operations may also be affected by India's relationships in the region. The sharing of information on a selective basis (whether by a regional ISC or by its partners) can also significantly undermine the ISC's intended role as a neutral information clearing house and can also distort trend analysis.

The stationing of ILOs at regional information-sharing centres involves significant investments from partner countries and represents a potentially valuable resource for regional cooperation. However, the effectiveness of ILOs can vary. They usually operate as individuals in a host country, with little guidance. Consequently, it has been observed that their performance (and therefore the quality of information shared with home agencies) will be proportional to their personal level of proactivity and dynamism. Overall, the ILOs stationed at regional centres do not always appear to be well-utilised.

In addition, in our view, communication methods that principally rely on ILOs are not sustainable in the long term. In general, the ILOs are provided with information by the IFCs that is then communicated with home agencies by email or messaging apps. Weekly and other periodic summaries are also prepared and distributed by email.

With the exception of the Singapore IFC, the regional information-sharing systems in the Indian Ocean do not provide a networked common operating picture that is available to national fusion centres of partner countries. The Singapore IFC offers the IFC Real-time Information Sharing System (IRIS) as a tool to provide a common operating picture for partners, although it is understood to be rarely used in practice.

Overall, reliance on ILOs as the principal channel of communications can significantly limit any potential utility of regional information-sharing centres as a source of real time operational intelligence for partner countries, although they remain a useful source of historical and contextual information.

This model for regional information-sharing is now facing significant disruption. Technological developments have led to a massive increase in data sources and analytical tools available to MDA users. Already, regional information-sharing centres such as Delhi IFC-IOR and Singapore IFC are the source of only a small proportion of operational information and intelligence used by partner countries around the Indian Ocean. That proportion is likely to fall in the future as MDA users gain greater access to networked information from international information and intelligence providers. This may require regional information-sharing centres to adapt to new roles.

Section 3: A new information-rich environment

We are increasingly seeing a new information- and intelligence-rich environment that will change the way MDA is done in the Indian Ocean and elsewhere in the Indo Pacific. Indeed, for the first time in history, the quantum of data, together with the use of automated analytical tools, has the potential to turn significant parts of the ocean into observed spaces.

Recent technological developments are producing vast amounts of data from new sources, including satellite sensors and, in the long term, a new generation of surface and undersea sensors. Another change is the availability of new automated analytical tools, including AI and machine learning (ML) tools, that can correlate and analyse multiple sources of data and detect anomalous behaviour. The amount of data that is becoming available in the maritime domain makes it particularly suitable for automated analytical tools.

Data from satellite-based sensing

The most obvious change in recent years has been a significant increase in access to satellite-based data, much of it from a plethora of new earth observation satellite systems, both government and commercial. As discussed previously, this includes data provided by several different types of sensors, including electro-optical imagery; Visible Infrared Imaging Radiometer Suite (VIIRS); radio frequency (RF) detection; and synthetic aperture radar (SAR).[23]

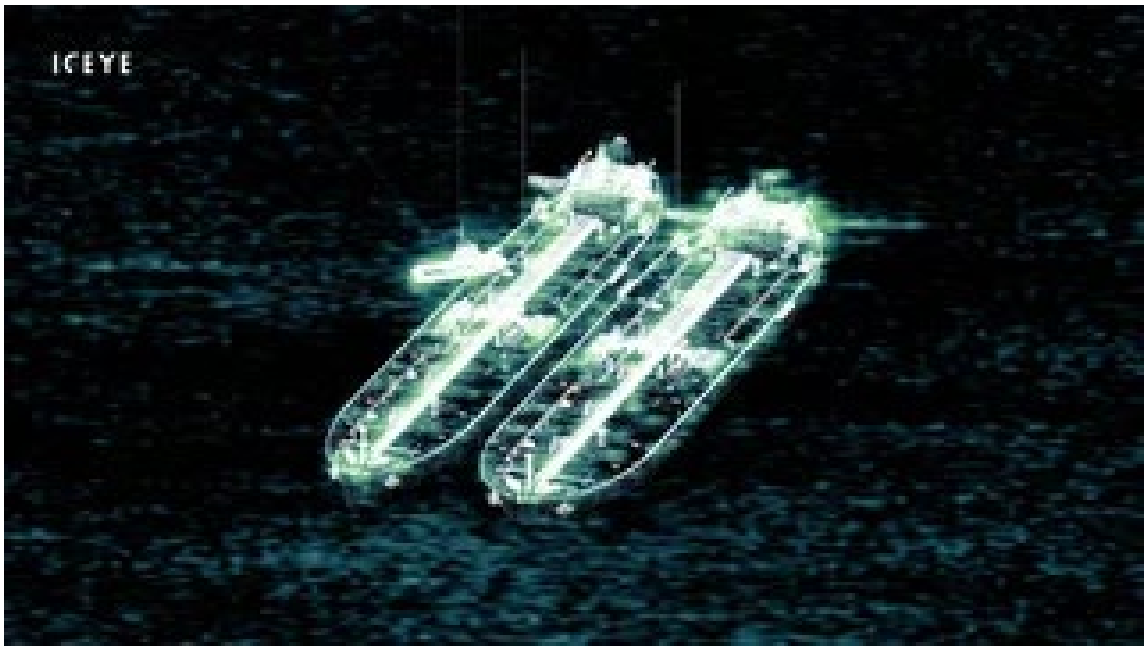


Figure 5. 'Dark rendezvous' transhipment by two tankers not emitting AIS signals, captured by SAR sensors and visualised in 3D. (Source: ICEYE)

These satellite-based sensors provide large amounts of data, sometimes at close to real time, making it much easier for MDA users to identify vessels of interest for further investigation. The satellites and their data are controlled and managed by many individual governments (e.g. Japan – JAXA, France – CLS) as well as commercial organisations (e.g. Airbus, UnseenLabs, ICEYE, PlanetSAT, HawkEye 360, Capella and UMBRA).

Although commercial satellite data has been historically expensive to access – and still is in many cases – access to data is improving due to the proliferation of small, low-cost satellites, many of them in low earth orbit. Data, particularly from satellites operated by governments, regional groupings or scientific organisations, can now often be acquired at relatively low or no cost. As an example, the US-based Skyfi company currently offers optical images of 25 km^2 areas at very high resolution (30-50cm per pixel) at US$300 per image for retail customers, or similar resolution SAR images at US$950 per image (see skyfi.com).

This trend of more easily available data at lower costs will likely be accelerated by the decision of the US National Oceanic and Atmospheric Organization (NOAA) in August 2023 to loosen national security-related licensing restrictions on US commercial remote sensing firms. While effectively opening up the customer base for space-based imaging firms, the rule change may be particularly important for operators of satellites with SAR.[24]

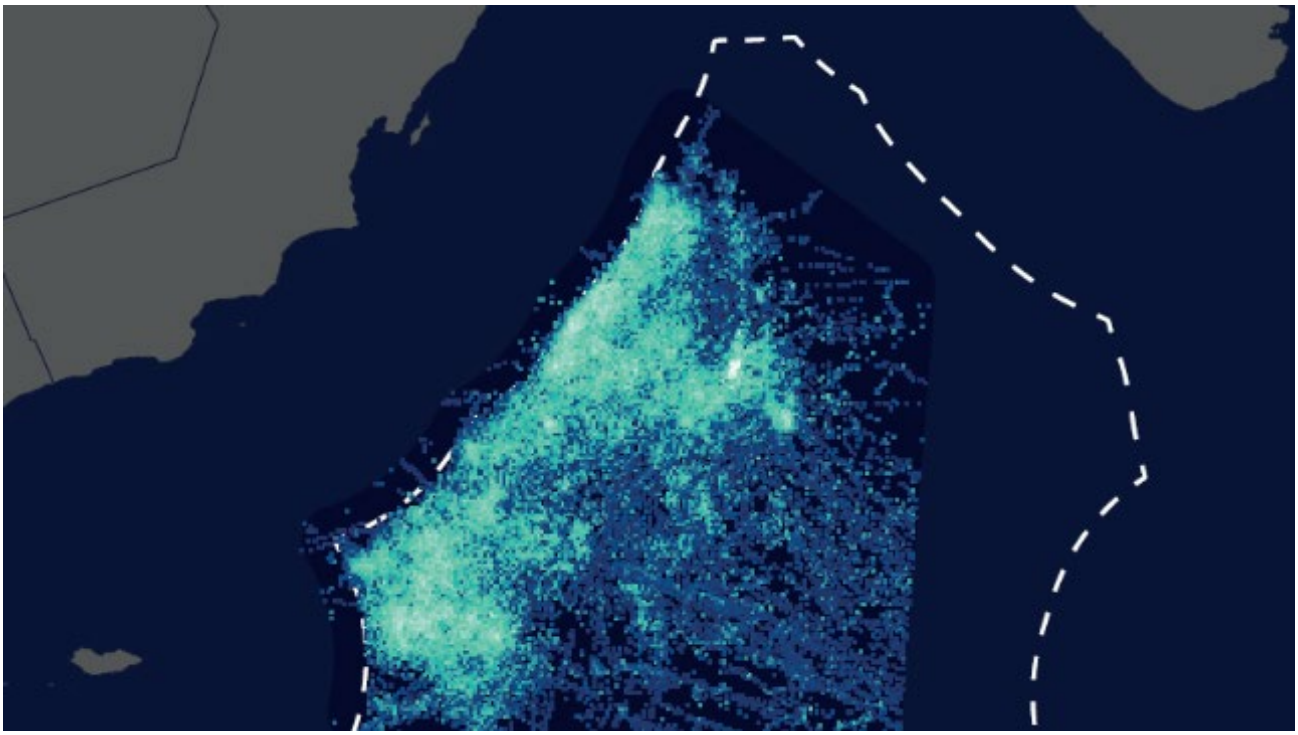


Figure 6: Chinese squid fishers off Oman captured on VIIRS sensors. (Source: Maritime Executive)

New analytical tools

The new generation of earth observation satellites produce far more data than human analysts could ever handle. Processing this data requires high-speed, high-volume computer analytic capabilities derived from image recognition and ML technologies that can process the data quickly enough to be useful for operational purposes. Satellites may also increasingly use onboard processing to reduce the need to transfer so much data. Big data analytics can also be used to make information useful for operational purposes, such as identifying links between a vessel of interest and its ultimate backers.[25]

Some benefits of these new analytical tools include improved threat detection and response times, more efficient resource allocation and enhanced decision-making processes. AI can also help support that ability of autonomous vessels and drones to operate autonomously, further improving surveillance and monitoring capabilities.

These new analytical tools are being developed not only by governments and large military contractors, but also by a range of actors that include NGOs, academics and start-ups, making them increasingly accessible.

These tools can be used to correlate and analyse multiple sources of data and detect anomalous objects or behaviour. This makes these tools useful for say, spotting a capsized fishing boat in a search and rescue operation, or for spotting potential vessels of interest that are not behaving in accordance with normal 'patterns of life'.

There are two basic approaches to detecting anomalous behaviour of vessels. The 'Exception from the Modelled Normal Behaviour' approach is usually used to build models of normal vessel behaviour from historical data. These models are then used to classify new vessel observations as normal or anomalous. They generally estimate the degree of deviation of a new target from the learned model of normal positioning/location, speed or trajectories.

Another approach is the 'Defining Anomalous Behaviour' approach which uses as a starting point some elementary base facts about the movement of vessels at sea. For example, the majority of vessels, especially in the open sea, seek to optimise fuel consumption by manoeuvring very little and keeping their speed constant. Vessels navigating in deep waters rarely perform manoeuvres in order to reduce ship trajectories into a sequence of waypoints. A vessel's pattern is made of events that tend to repeat in a specific timeframe and predictable manner. For example, while heading towards a fishing zone, one pattern may be normal for a fishing boat, but should be marked as anomalous for a tug boat.

For example, *Global Fishing Watch,* working in conjunction with several non-governmental partners, uses a ML model applied to its comprehensive vessel registry database to classify vessels into one of 40 vessel categories such as trawler, longliner or cargo. ML models then use vessel-tracking datasets (AIS/VMS), along with the classification data, to identify when and where a vessel is fishing based on its movement patterns. For satellite imagery, 'object detection' models are used to distinguish vessels from other objects.

These new tools are also used to identify vessels that are 'spoofing' their GPS or transmitting a MMSI not assigned to them. ML algorithms will automatically separate signals coming from multiple vessels using the same MMSI, and also detect when the broadcast location is inconsistent with the location of the satellite that detected the signal.[26]

Data from surface and undersea sensors

In future, we should expect that large amounts of satellite-based data will be supplemented by large amounts of data from new surface and undersea sensors – again, from a combination of government and non-government providers. Like data from earth observation satellites, this data will likely initially be largely available to more developed countries, becoming progressively more accessible to more users as the number of sensors proliferate.

Data from the ocean surface will be driven by the proliferation of buoys and uncrewed surface vehicles (USVs) operated by state agencies and scientific and commercial operators. There are many startups operating in this space, such as the United Kingdom-based company Oshen, which has developed tiny autonomous sailboats that can be steered on selected courses, unlike floating buoys that generally cannot be steered.[27]

The US-based Saildrone already deploys a fleet of dozens of USVs with hull lengths of 10m and 20m, primarily using sail propulsion with back-up diesel or electric propulsion. They have a cruise speed under sail of 5-6 knots and a listed endurance of more than three months. They can be fitted with payloads of active and passive sensors for a range of applications including defence, law enforcement and ocean mapping. The USVs are operated remotely by Saildrone, which then sells the data. In 2019, a Saildrone USV circumnavigated Antarctica over a period of more than six months.

The US Navy and others have been experimenting with using multiple Saildrone USVs in a networked manner for surveillance in the Persian Gulf (which included an attempt by Iranian vessels to interfere with a Saildrone in 2022).[28] In January 2024, the Bahrain-based US Naval Task Force 59, stood up a new Task Group 59.1, which is focused on the operational deployment of uncrewed systems in the northeast Indian Ocean.[29]

In future years, we should also expect a significant increase in data on the undersea environment from the proliferation of new undersea sensors. Undersea cables have the potential to be transformed into undersea sensor arrays. Environmental sensors are being installed inside repeaters for undersea communications cables as part of the Science Monitoring and Reliable Telecommunications (SMART) cables initiative. In 2012, UN agencies, including the International Telecommunication Union, the IOC, and UNESCO established the Joint Task Force on SMART cable systems.[30] Scientific use cases include sustained ocean observation and earthquake/tsunami warning and climate monitoring.[31]

Cable-mounted sensors can also be used to monitor underwater vehicles, as modern equivalents of the Cold War era Sound Surveillance System (SOSUS) operated by the US. These have already been deployed in some parts of the world. Indeed, in 2021 a Norwegian submarine detection system was reportedly disabled, presumably by Russian actors.[32]

It is also likely that, in the long term, data from fixed undersea sensors will be complemented by uncrewed underwater vehicles (UUVs), including wave gliders. After originally being used for mine warfare, UUV technology is advancing to the point where they can be used for long-range missions. Pressure-tolerant L-ion batteries can power operations for up to 15 days without the support of a mothership. For missions of this length, AI is utilised to deal with the complexities of changing tides, currents, topographical disturbances, pressure changes and weather effects. AI can interpret volumes of data, imitate human intuition and make decisions on manoeuvrability and respond to failures. This technology is still in the testing phase and it will likely be some years before it becomes widely available. It is likely that data from UUVs will initially be available only to advanced actors who may choose to share it with regional partners with less developed capabilities.

Section 4: Web-based Information-sharing Platforms

Another significant new technological development is the growing availability of online information-sharing platforms that allow MDA users around the region to directly access satellite-based sensors and other data from multiple sources. They are often used by national information fusion centres and maritime enforcement agencies to develop common operating pictures, generally based on AIS data that is overlaid with satellite-based and other data. The correlation of this data, along with analysis of vessel behaviour, helps users to identify vessels of interest that may require further investigation.

SeaVision

One of the most prominent web-based platforms used by Indian Ocean countries is the US government-sponsored *SeaVision* platform, operated by the US Department of Transport.

SeaVision is a web-based maritime domain awareness tool that enables users to view, analyse, and share a broad array of maritime information. It builds on basic AIS data with overlays of satellite data (which may include SAR, VIIRS and RF), and proprietary vessel data obtained from private and public satellite systems from the US, Europe and elsewhere. This allows users to identify so-called 'dark' vessels that have switched off or spoofed their AIS devices and build an understanding of the activities of dark vessels.

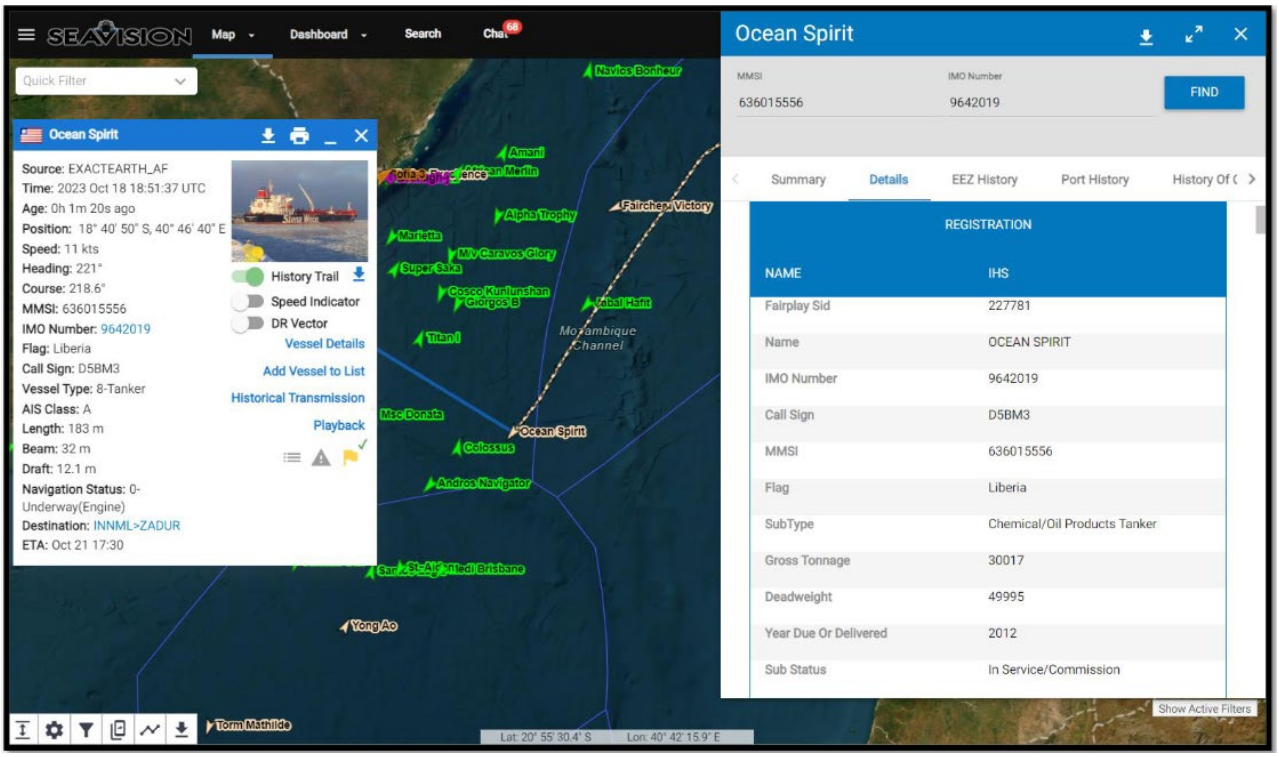


Figure 7: Screenshot from SeaVision

The identified strengths of the system include real-time vessel and domain monitoring, maritime analysis and establishment of a common operating picture. Identified weaknesses include its inability to support secure direct peer-to-peer communications between users. In other words, all user-generated data and communications made through the *SeaVision* system is visible to the US sponsors.

The US has already provided *SeaVision* with satellite overlays to dozens of partners throughout the world. The system is now being provided at no cost to a number of Indo-Pacific countries pursuant to the Quad's Indo-Pacific MDA (IPMDA) Initiative announced in May 2022. Under the IPMDA, *SeaVision* is being provided with satellite data, including *HawkEye 360,* plus information from *Skylight*. Because of its commercial origin, this data is unclassified, allowing the Quad to provide it to a wide range of partners.[33]

The initial geographic focus of the IPMDA was in providing *SeaVision* together with training to Southeast Asian and Pacific partners. It is understood that Australia is funding the costs of *HawkEye 360* data for Pacific partners. In July 2024, the Quad Foreign Ministers announced they intended to expand the IPMDA initiative to the Indian Ocean region, including the early operationalisation of the South Asia program.[34]

IORIS

Another prominent platform is the Indo-Pacific Regional Information Sharing (IORIS) platform, which is provided to Indo-Pacific countries under the European Union-sponsored CRIMARIO II program. *IORIS* also provides basic AIS data with satellite overlays, including the *Skylight* product. Although there are similarities between *IORIS* and *SeaVision*, there are important differences. CRIMARIO acknowledges the data limitations of *IORIS* and promotes the system principally as "a web-based communications tool that provides command and control functions to plan and coordinate maritime operations with the infusion of very limited satellite data".[35]

The strengths of the *IORIS* system lie less in the AIS/satellite-based data provided through the system (which is somewhat limited) and more in its value as a system for the coordination and communication for incident management between enforcement and safety agencies in the same country (e.g. navies and fisheries enforcement) or between the same agencies in different countries.

The *IORIS* system allows for the creation of what could be described as secure 'chat rooms' (either permanent or ad hoc) between agencies that facilitate coordination in response to particular regions or particular incidents. These chat rooms allow participants to share user-generated data and intelligence in a secure manner via the cloud (Microsoft-Azure server in South Africa), without the involvement of the system sponsor. In essence, the *IORIS* system allows self-selecting participants to create their own, shared, common operating picture including their own data in a way that is particularly useful for facilitating coordinated responses between countries.

Figure 8: Screenshot from IORIS. (Source: CRIMARIO II)

The *IORIS* system is made available to low- and middle-income Indian Ocean countries at no charge, although high-income countries are required to pay moderate fees. The UN Office of Drugs and Crime (UNODC) plays an important role in facilitating *IORIS* access and training for maritime law enforcement agencies throughout the Indian Ocean region. CRIMARIO II has a policy of trying to make the system self-supporting through regional groupings that govern the use of the system in their areas.

Although some might initially see *SeaVision* and *IORIS* as competing platforms promoted by the US and Europe, that is not necessarily the case. In practice, most Indian Ocean countries tend to use both systems, but for somewhat different purposes. *IORIS* is used principally as a communication tool, while *SeaVision* is used for surveillance and data analysis.

It would be of significant benefit to MDA users in the Indian Ocean and elsewhere if the US, the EU, India and others could overcome bureaucratic barriers to make the regional/national systems interoperable. CRIMARIO II has also developed a system called 'SHARE.IT' that would facilitate linking different information exchange platforms, including but not limited to *IORIS* and *SeaVision,* to facilitate the exchange of information and data in a structured and secure manner.

The sponsors of *IORIS* and *SeaVision* have developed a so-called 'non-paper' that emphasises the complementarity of the two systems (the non-paper is set out in Appendix 2). Nevertheless, countries such as India and Australia have refused to use the *IORIS* system for reasons that may be more political than practical. Australian representatives attended the last SHARE.IT conference in Bangkok co-organised with UNODC and relevant Australian agencies are understood to be following concept's development.

Other web-based products and platforms

These major state-sponsored platforms are also being supplemented by many other web-based maritime information and intelligence products, including many provided by NGOs and private companies, some of which are described below.

There are many companies providing satellite imagery on a commercial basis, often at considerable cost. These include Planet, Maxar, ICEYE and Unseen Labs. One prominent commercial provider is *HawkEye 360*, which offers a range of MDA products, including satellite-based radio frequency data to help identify so-called dark vessels. Figure 9 shows the potential value of *HawkEye 360* RF data by showing the differences between AIS-reported locations and X-band marine radar geolocations in the South China Sea. *HawkEye 360* products are provided to *SeaVision* users in various access levels as part of the Indo-Pacific MDA Initiative, although it is constrained by the costs *Hawkeye 360* charges.

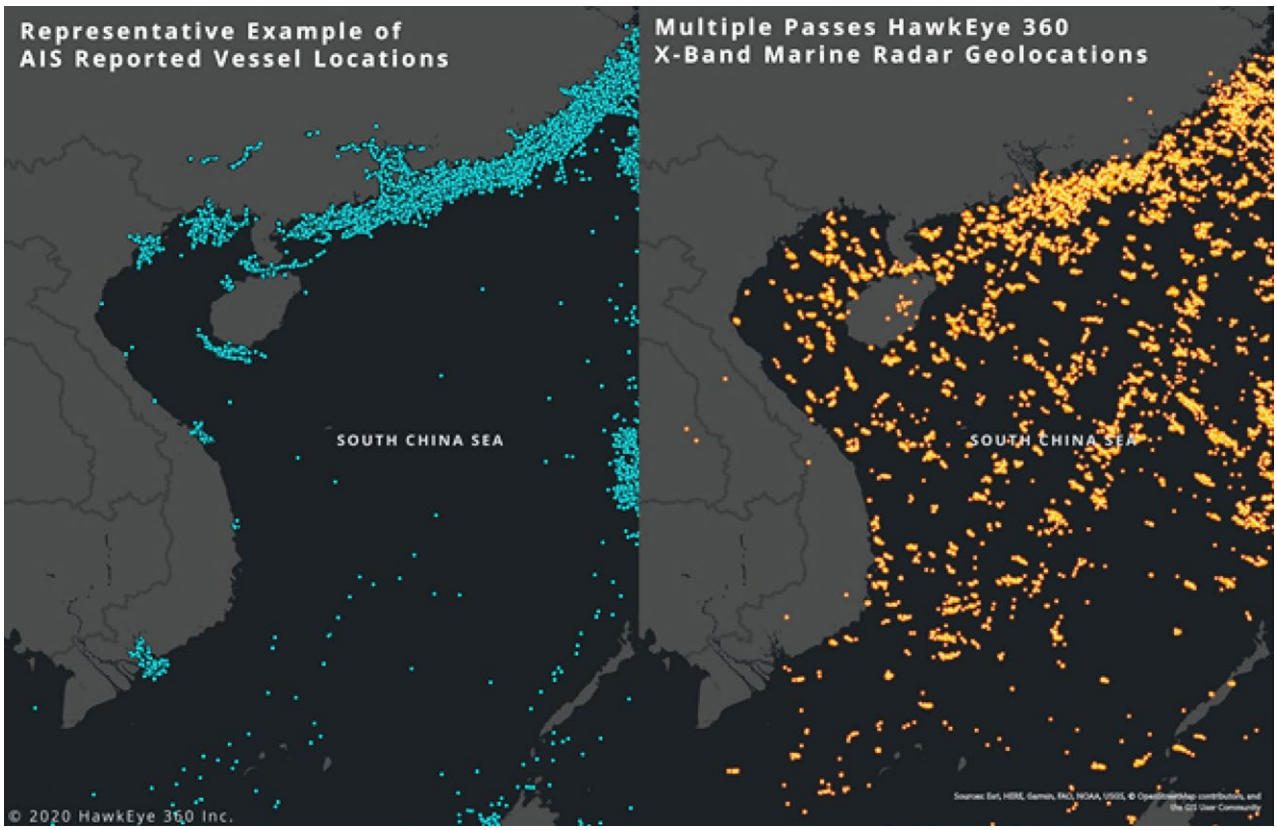


Figure 9: Differences between AIS-reported locations and X-band marine radar geolocations in the South China Sea, as detected by HawkEye 360 (Source: HawkEye 360)

Another popular product is *Skylight*, provided to users at no cost by the Allen Foundation, an NGO funded by the estate of Microsoft co-founder Paul Allen. Originally established to monitor and prevent IUU fishing, *Skylight* uses data from multiple free sources. These include AIS and the European Sentinel 1 and 2, and Night Lights satellites. *Skylight* also acquires data from its commercial partners Spire and Maxar. Together, these provide a combination of actual positional data and information obtained from optical, SAR and RF sensors. *Skylight* then applies AI algorithms through this enormous amount of data before producing operational intelligence on dark vessels and dark rendezvous, sometimes within minutes, facilitating real-time operations. While the original intent of *Skylight* was the prevention of IUU fishing, it now has proved to be an extremely useful tool that can be used for all aspects of MDA at a cheap price.

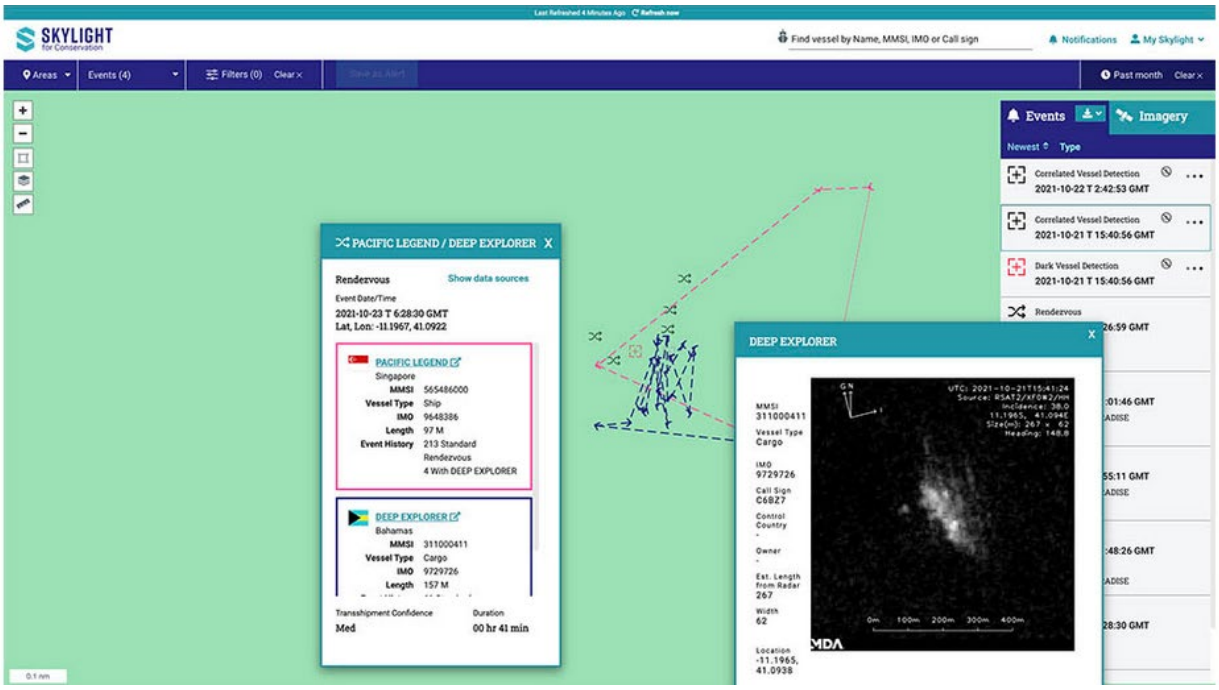


Figure 10: Screenshot from *Skylight* analysing a possible transshipment between two AIS transmitting vessels. In this case, Skylight shows a correlated vessel between AIS signal and a satellite image (SAR) of the vessel *Deep Explorer*. (Source: Spire.com)

Global Fishing Watch (GFW) is another NGO that has made considerable advancements with its MDA capability. GFW works as part of the Joint Analytical Cell with other NGO partners such as TM-Tracking,[36] the International Monitoring, Control and Surveillance Network,[37] *Skylight* and c4ads.[38] Like the *Skylight* platform, GFW compiles data from several sources including AIS and satellite sources, as well as Google Earth. GFW also has access to VMS data from several countries that have made this data available to the GFW map – a major addition given the large number of fishing vessels that may transmit on VMS but not AIS. Additionally, GFW synthesises data from 30 public vessel registries each month to develop a comprehensive database of known vessel information, including identity — ship name, call sign, IMO number, size, length, tonnage, engine power, authorisation status and ownership. Algorithms and machine-learning models are then applied to this data to monitor the activities of fishing vessels at sea.

Indian Ocean countries may also have access to state-sponsored platforms other than from the US and EU. This includes the Canadian Dark Vessel Detection (DVD) Program, which has recently been used prominently by the Philippines in the South China Sea. This was developed by the Canadian Government, principally for the detection of illegal fishers using satellite data, including RF, SAR and base geo-spectrum imagery.

Several companies also offer what might be described as 'maritime intelligence' products. These include Windward, a 'predictive intelligence company' with ties to Israel and the UK, which specialises in providing intelligence to the commercial shipping industry on subjects such as the behaviour of commercial vessels, vessel safety, logistics and sanctions.[39] Windward claims that its AI model continuously trains on a database of hundreds of historical records of vessels engaged in criminal activities. According to Windward, this means that unique behavioural events, like drifting speed, ship-to-ship (STS) meetings, first-time visits, and location tampering, are all evaluated in the context of their security risk.

Another commercial maritime intelligence provider is Starboard, a New Zealand-based company that specialises in biosecurity and fisheries surveillance.[40] Starboard takes AIS data on fishing vessels together with satellite sensing (optical, RF and SAR) and assesses vessel behaviour. Starboard also applies a bespoke risk model to the vessel based on its history, port visits and any history of anomalous vessel movements. Although both Windward and Starboard provide intelligence on a fee-for-service basis, they also make certain products available to selected clients on a free or discounted basis.

Several maritime security companies also conduct data analysis, including Ambrey and Risk Intelligence. The data is used to inform risk decisions ahead of possibly providing maritime security teams on board ships.

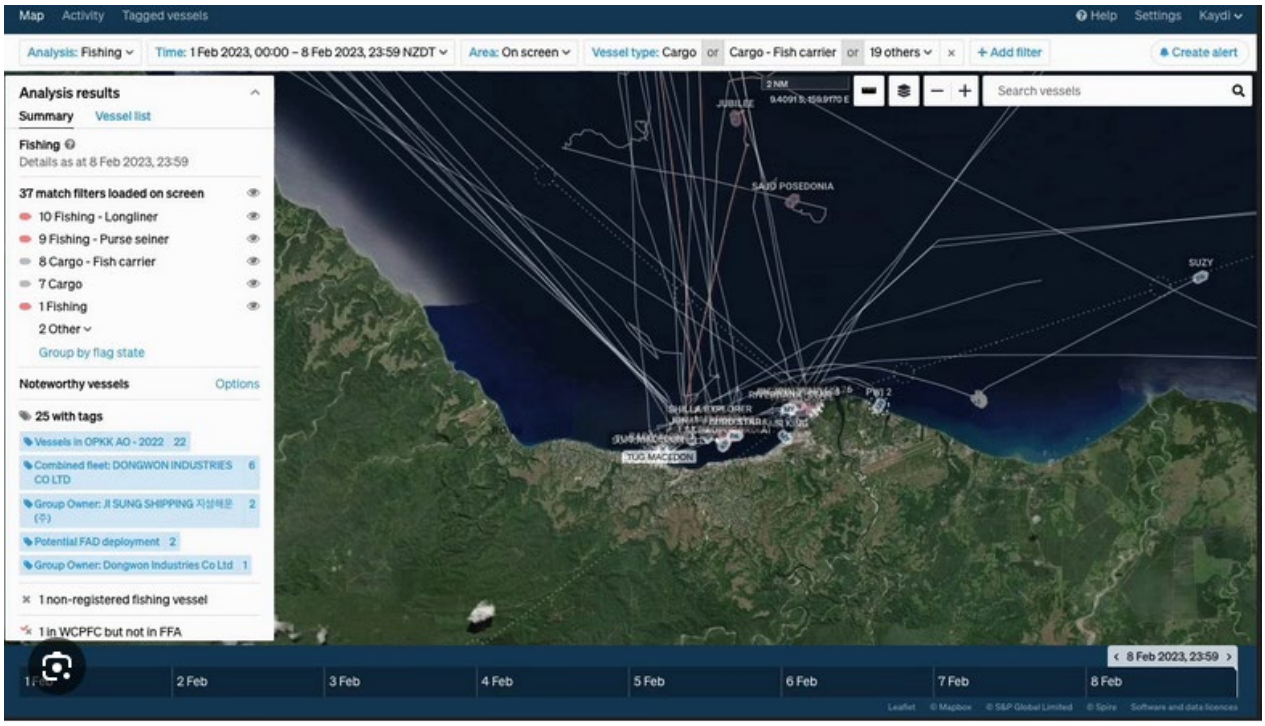


Figure 11: Screenshot from Starboard showing analysis of fishing activity. (Source: Starboard.co.nz)

Collectively, these platforms and products have the potential to provide MDA users with a virtual firehose of data and intelligence. However, smaller and less developed countries in the Indian Ocean may struggle to take full advantage for several reasons, including cost, lack of appropriate analytical skills and the disaggregated nature of these platforms and products.

Section 5: The future of MDA information- and intelligence-sharing arrangements in the Indian Ocean

This section considers what these developments mean for the future shape of maritime information- and intelligence-sharing arrangements in the Indian Ocean and elsewhere in the Indo-Pacific.

Implications for MDA users

A new information-rich environment in the Indian Ocean will have significant implications for users of maritime information and intelligence, giving them more options than ever before.

Diversity of information sources: For one thing, MDA users will have much greater access to information from a wide range of potentially diverse sources. This would facilitate cross-checking of data provided by different partner countries and commercial providers, reducing concerns about relying on information from a single source. The growing ability to cross-check data could actually enhance trust in information supplied by larger partners.

Increased reliance on open-source information: There will likely be increased reliance on open-source information, including from private companies and NGOs as well as state-sponsored platforms such as *SeaVision* that incorporate private data sources. The virtual monopoly that government agencies (particularly navies) have long had in MDA is under significant challenge.

While these new sources of information may still be formally classified as 'open-sourced', it should not be assumed this means that such information is easily available. Indeed, the Cold War era term of 'open-source' is increasingly unhelpful in describing how practically available such information actually is. Cyberspace is increasingly fragmented and commercial information providers, whose capabilities may increasingly match or exceed those of nation states, may charge fees that are greater than many countries can realistically afford.[41]

Nevertheless, it is clear that the proliferation of new 'open-source' information will likely lead to a relatively reduced reliance on information from secret sources for the purposes of maritime law enforcement. A transition from a traditional naval intelligence system to a quasi open-source system will involve many considerations that still need to be worked through. This is part of a broader challenge of how open-source intelligence should be integrated into information and intelligence systems.

Lack of secure communications: Many maritime enforcement agencies in the Indian Ocean region use non-secure computer equipment and communications systems (including WhatsApp), creating information security concerns vis-a-vis state-based actors and even organised crime groups. But the challenge of creating a region-wide secure communications system is great. Should it be simply assumed that maritime information shared by these means is unlikely to be secure? Do we need to accept that information may be secure only for immediate purposes?

Importance of analytical capabilities: The growing availability of online analytical tools, properly used, will likely also change the roles of human analysts. Nevertheless, the volume of data will still likely place significant strain on analytical capabilities of Indian Ocean countries, which are in some cases already very thin. This means that there needs to be greater focus on building MDA analytical skills among Indian Ocean partners.

With properly trained analysts, timely maritime intelligence, particularly operational intelligence, may be the product of, say, a naval lieutenant with a laptop rather than traditional large operations rooms. However, this in turn may also require greater oversight and verification of analytical outcomes.

Democratisation of information and intelligence: For smaller or less wealthy countries around the Indian Ocean, the proliferation of alternative information-sharing systems can be an important way of democratising maritime information and intelligence, meaning that they are less reliant on large countries. Sri Lanka, for example, is the biggest country user of the privately operated *Skylight* system. Indeed, web-based platforms could allow such countries to leap-frog the older and expensive 'bricks and mortar' systems by giving users timely access to high-quality operational intelligence at lower cost.

The future of information- and intelligence-sharing may be more federated than hierarchical in nature, giving smaller or less developed countries more autonomy in decision-making than might otherwise be the case.

Growing pressures on response capabilities: The availability of large amounts of networked maritime information and intelligence has the potential to revolutionise MDA, making broad swathes of the ocean observed spaces for the first time. This, in turn, may place greater pressure on countries to have better response capabilities than they currently have and may be beyond the resources of many smaller or less wealthy countries. (Indeed, some observers have commented that maritime enforcement agencies in some countries may find it convenient to not be aware of some activities occurring in their maritime jurisdictions.)

One solution to increased pressures to respond to identified threats may be to enhance regional cooperation arrangements to respond to identified threats. The 'federated' system of threat response being developed at the Regional Coordination Operations Centre in Seychelles could provide an interesting model for the effective pooling of response capabilities. The cooperative enforcement system used by the Pacific Islands Forum Fisheries Agency in Honiara to enforce fisheries management for FFA member states could also provide a useful model for Indian Ocean states.[42]

Implications for Australia

Focus on building national capabilities of selected Indian Ocean partners: Australia has strong interests in seeing Indian Ocean states build their sovereign national capabilities to provide maritime security in their areas of national jurisdiction and beyond. Australia has been working with Indian Ocean states such as Bangladesh, Sri Lanka and Maldives to help improve their maritime capabilities, including in MDA, in accordance with their own national needs and priorities. In doing so, Australia has the benefit of generally being seen as a trusted regional partner.

However, Australia will have only limited resources to invest in these Indian Ocean partnerships, especially given competing priorities in the Pacific and Southeast Asia. This means that Australia will need to leverage its own expertise in MDA, as well as working with like-minded partners to provide focused solutions to the new information-rich environment at low cost.

Evolution of Common Information Platform: As a Quad partner, Australia also has significant interests in the seeing *SeaVision*, or a newly developed platform, being adopted as a common and trusted information platform by many Indo Pacific countries. This includes providing significant financial support for Pacific Island countries to access commercial information through *SeaVision*.[43]

One answer to the cost problem could involve the better integration of open-source products into a common information platform operated in public-private partnership. The involvement of private companies in such a platform may provide opportunities to significantly mitigate costs.

SeaVision and IORIS: Australia also has an interest in promoting the use of *SeaVision* and *IORIS* by regional partners as complementary and not competing platforms. Australian agencies such as Australian Border Force, the Australian Maritime Safety Authority and the Australian Fisheries Management Authority, should be permitted to use *IORIS* as a communications platform with relevant Indian Ocean partners if they are in a position to pay for access.

Support for regional groupings: Australia can also provide further diplomatic support for the work of Indian Ocean regional groupings such as the Indian Ocean Rim Association (in which Australia acts as co-chair of the Maritime Safety and Security Working Group), Indian Ocean Naval Symposium and BIMSTEC to promote the value of sovereign national MDA capabilities alongside regional maritime information-sharing arrangements.

Take the lead in niche MDA areas: Australia could consider taking a leading role in niche MDA areas, which could include creating information-sharing and response networks with selected Indian Ocean partners. These could involve the specialist Australian agencies such as Cyber and Infrastructure Security Centre (Home Affairs) and the Cable Connectivity and Resilience Centre (DFAT). There is also considerable scope in Australia taking a leading role in organising regional arrangements for environmental monitoring and response, including oil spill monitoring and response, leveraging the expertise of several Australian agencies in these areas.[44]

Help build analytical capabilities: As previously noted, the deluge of data is placing significant strain on human analysts in many Indian Ocean partners, even with the availability of new analytical tools. Australia could also make a valuable contribution in helping selected Indian Ocean partners build their MDA analytical capabilities, including training in the use of automated analytical tools.

Consequences for regional information-sharing centres

Need to adapt roles and networking arrangements: Regional information-sharing centres will necessarily need to adapt to this new information rich environment. In many cases they may find it difficult to compete directly with online platforms as sources of operational information or intelligence for MDA users unless they change current practices. The lack of a networked common operating picture and their reliance on communication through ILOs does not provide an optimal solution for national MDA users looking for real-time or near real-time operational information. Already the regional fusion centres supply only a small proportion of the operational information and intelligence used by national maritime authorities, and that proportion is likely to fall.

Valuable sources of strategic intelligence: Regional information-sharing centres may still play key roles in the future MDA architecture of the Indian Ocean region. Notwithstanding their future role in providing operational information and intelligence, they could remain a highly valuable source of strategic intelligence. That is, they could be a source of historical information used in tracking and understanding broad trends in regional threats, much like the role played by the Pacific Fusion Centre in Vanuatu.[45]

Improved use of International Liaison Officers: The presence of ILOs at regional information-sharing centres also provides many opportunities that may not have been properly explored. ILOs are seen as conduits of data to and from partner countries and appear to be under-utilised. The presence of large numbers of ILOs in Delhi, Singapore, Madagascar and Seychelles is a potentially highly valuable resource, and their roles could be expanded more towards regional liaison and multilateral response coordination and other roles.

Organising for a new information-rich environment

The growth of a new information-rich environment involving the diversification of information sources and the development of new non-government platforms will have a profound impact on arrangements for the sharing of maritime information in the Indian Ocean and elsewhere in the Indo Pacific. There are several challenges and concerns.

Integrating open-source information: Some may remain suspicious of the proliferation of new open-source information products, driven by concerns about information security, a wish to promote national systems, or for other political reasons. There is no doubt that non-governmental information providers — whether for-profit providers or NGOs — have their own interests and agendas. However, any temptation to tamper with data may be constrained by the great diversity of information providers and the ability of users to compare and correlate data from different providers. Indeed, in some cases, smaller countries may be inclined to place greater trust in publicly available information compared with information supplied to them by larger countries. This is part of a broader discussion of the role of OSINT in national intelligence systems.[46]

Continued importance of human intelligence: There will be no single answer to the challenge of establishing effective MDA, and users will still need to access information of many different types**.** The ease of use and apparent comprehensive nature of information from these new platforms should not, for example, overshadow the importance of human intelligence, which can be crucial in *understanding* the behaviour of maritime actors. Fishers or coastal communities will often have a deep understanding of the patterns of life of maritime actors that cannot be replicated by technology.[47]

Since 2015, the Australian Government has operated an Indigenous Ranger Biosecurity Program involving a network of indigenous ranger groups across Northern Australia.[48] In recent times, there have also been several instances where Indigenous people have alerted Australian authorities to illegal maritime arrivals that had not been detected by high-tech surveillance methods.[49] Similarly, the network of Coast Observation Posts around Sri Lanka, operated by the Sri Lanka Navy, provides a unique and highly valuable communications link between coastal fishing communities and maritime enforcement authorities.

Need for a common open-source information platform: Although the proliferation of new data sources is generally a positive development, many MDA users already struggle with fusing and analysing different sources of data provided through different platforms. There is a real need for a single platform that can be used to effectively aggregate, correlate and analyse different sources of data in accordance with the requirements of particular MDA users.

Although *SeaVision* and *IORIS* are both moving in that direction, they are not currently providing the products that many MDA users need, and there are questions over whether they can evolve quickly enough.

uld be to seek to develop a common MDA information-sharing mechanism through a multilateral MDA 'framework' that brings together larger or advanced countries with developing countries.[50] This would involve the harmonisation of existing regional MDA initiatives and the development of shared norms and practices. It would also involve a recognition that while more advanced countries may be able to assess large amounts of data using advanced analysis tools, they might not be able to connect the patterns they find since they may lack the local shipping awareness that smaller countries might have.

But a multilateral solution to the MDA problem would likely have significant problems. Region-wide multilateral arrangements are not known for their ability to quickly develop innovative solutions, and they can be easily derailed. China, for example, may not think it is necessarily in its interests that its vessels can be more easily tracked by maritime law enforcement of smaller neighbours, and may choose to block (directly or indirectly) any multilateral regional efforts in this area.[51]

The Quad IPMDA may provide an alternative avenue for the development of a multilateral-style common open source information platform. The US-sponsored *SeaVision* platform, offered by the US as part of the IPMDA initiative, may provide a useful stopgap platform, but its functionality is limited and its heritage and system architecture (in which the US has access to all information) creates sensitivities among many MDA users in Indian Ocean states.

There may be potential for the Quad partners to evolve *SeaVision*, or even better, create a new platform, that is perceived to be more multilateral and transparent in nature. The objective would *not* be to create a universal common operating picture that is available to all MDA users, from the tiniest island state to major powers. The needs of MDA users around the Indian Ocean region are too diverse to demand such a result.

However, a useful — and achievable — objective would be to establish a common open-source information platform that allows governmental, commercial and NGO entities to 'plug and play' their information products, allowing MDA users to select from a menu of information products according to their needs and financial circumstances (including whatever subsidy arrangements they may have access to).

Such a common information platform would aim to provide users with an 'a la carte' solution to their MDA needs and would *not* seek to provide a universal common operating picture. This would reflect both the diversity of information sources and the diversity of information needs.

The management arrangements for such a platform would also need to take into account the political/geostrategic anxieties of many countries in the region, small and large. There may be potential to use a consortium approach involving civilian government agencies and, perhaps, private companies, that may go some way towards mitigating these anxieties. The presence of commercial information providers may also wholly or partly offset the costs of establishing the platform.

Appendix 1 – Glossary

ABOC	Australian Border Operations Centre
AI	Artificial Intelligence
AIS	Automatic Identification System, an automated vessel tracking system mandated by international law for certain vessels
COP	Common Operating Picture
CRIMARIO II	Critical Maritime Routes Indo-Pacific project, a regional maritime security capability building program sponsored by the European Union
IFC-IOR	Information Fusion Centre-Indian Ocean Region, located in Gurgaon, India, and operated by the Indian Navy
ILO	International Liaison Officer
IMAC	Information Management and Operations Centre, operated by the Indian Navy
IPMDA	Indo-Pacific Maritime Domain Awareness initiative, an initiative of the Quad partners to enhance MDA in the Indo Pacific
IORIS	Indo-Pacific Regional Information Sharing system, operated by CRIMARIO II program and sponsored by the European Union
IRIS	Real-time Information Sharing System
ISC	Information-Sharing Centre
LRIT	Long-Range Identification System, an automated vessel tracking system mandated by international law for certain vessels
MDA	Maritime Domain Awareness
MOC	Maritime Operation Centre
OSINT	Open-Source Intelligence
RCOC	Regional Coordination Operations Centre, located in Seychelles
RF detection	Detection of radar and radio emissions
RMICF	Regional Maritime Information Centre, located in Madagascar
SAR	Synthetic Aperture Radar, a type of radar that can be used on earth observation satellites to detect vessels
SeaVision	A web-based MDA tool that enables users to view, analyse, and share a broad array of maritime information that is sponsored by the US Department of Transport
SHARE-IT	Sharing and Enhancing Information and Technology, a framework developed by CRIMARIO II to link existing information exchange systems
Singapore IFC	Information Fusion Centre, located in Singapore and operated by the Singapore Navy
VIIRS	Visible Infrared Imaging Radiometer Suite, used on earth observation satellites to detect light emissions
VMS	Vessel Monitoring System, an automated vessel tracking system mandated by some countries to track commercial fishing vessels
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle

Appendix 2 – SeaVision-IORIS Non-Paper

The *SeaVision* and *IORIS* Platforms: Complements, Not Competitors

This non-paper compares and contrasts the major features of the U.S. Department of Transportation's **SeaVision** maritime domain awareness (MDA) platform and EU-funded project CRIMARIO II Indo-Pacific Regional Information Sharing (**IORIS**) platform, highlighting how they can be used in combination. This is a high-level overview that glosses over nuances and caveats. Prospective users of either platform should conduct additional research and must consider their contextual particulars. Additional links are included at bottom to help determine the best approach.

	SeaVison	**IORIS**
Overview	A web-based maritime domain awareness tool that enables users to view, analyze, and share a broad array of maritime information	A web-based communications tool that provides command and control functions to plan and coordinate maritime operations with the infusion of very limited satellite data
Use Case Strengths	Real-time vessel and domain monitoring; maritime analysis; establishment of a common operating picture (COP)	Coordination and communication for incident management through a dedicated COP with collaboration spaces and document preservation, including for legal finish
Features	Track fusion and visualisation, analytic tools, historic tracks, alerts to phone, chat, and a mobile version	Message, chat, notifications, VOIP, file- sharing/archiving, and mapping functions
User / Collaboration Space Management	SeaVision Community Managers actively manage user roles in defined Communities and Portfolios	Any user is able to create Community Areas for sustained efforts or for an ad-hoc basis
Costs to Users / Availability	None / Available globally to sponsored government users	None for low and middle-income countries / Available to all countries in the Indo-Pacific
Data	Dependent on user Communities / Portfolios and associated data licenses. May include AIS, SAR, Radar, VIIRS, RF, proprietary vessel data, user-provided Skylight overlay	User-provided. Platform includes baseline AIS and other limited data sources for coordination of specific operations (not 24/7). Users may add any other data. Skylight overlay
User-Provided Data Protection	Data is only shared with others within agreed-upon designated Portfolios	Only users in Community Areas have access to information shared, which excludes CRIMARIO, unless invited for mentoring purposes

Vignette

A watchstander at a nation's maritime law enforcement agency operations center monitoring *SeaVision* receives an algorithm-generated alert that a tracked vessel may be engaged in fishing activity in a user-defined geographic area, in this case correlating with a no-take marine protected area. The watchstander uses *SeaVision* to check the vessel's track history and determines that the vessel also likely performed a transshipment with another vessel. The watchstander alerts their command, which calls POCs in the Ministry of Justice and the Ministry of Natural Resources, notifying them that they will begin coordinating a response via IORIS. The watchfloor uses IORIS to create a Community Area dedicated to the incident, inviting their inter-governmental partners to it to exchange information and documents about the vessel and to communicate decisions regarding enforcement actions – permanently preserved for later review by the parties involved. Decision-makers may then opt to exchange information with neighboring countries using *SeaVision* or *IORIS*.

Additional Information:SeaVision: https://info.seavision.volpe.dot.gov/

IORIS: https://www.crimario.eu/ioris-the-maritime-operational-coordination-communications-platform-for-the-indo-pacific/

Endnotes

1 David Brewster, *Australia's Second Sea: Facing our Multipolar Future in the Indian Ocean,* Australian Strategic Policy Institute, 2019. https://www.aspi.org.au/report/australias-second-ea-facing-our-multipolar-future-indian-ocean, accessed 6 September 2024.

2 Penny Wong, 'Keynote Address to the 7th Indian Ocean Conference' Perth, 7 February 2024. https://www.foreignminister.gov.au/minister/penny-wong/speech/keynote-address-7th-indian-ocean-conference, accessed 6 September 2024

3 David Brewster, Anthony Bergin and Aakriti Bachhawat, *Ocean Horizons: Strengthening maritime security in Indo-Pacific island states*, Australian Strategic Policy Institute, 2019.

4 See generally, David Brewster, 'Give light, and the darkness will disappear: Australia's quest for maritime domain awareness in the Indian Ocean,' *Journal of the Indian Ocean Region* (2018), Vol.14, No.3, pp.296-314.

5 Under Safety of Life at Sea regulations, AIS must be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size. The regulation requires that AIS shall: (i) provide information — including the ship's identity, type, position, course, speed, navigational status and other safety-related information — automatically to appropriately equipped shore stations, other ships and aircraft; (ii) receive automatically such information from similarly fitted ships; (iii) monitor and track ships; and (iv) exchange data with shore-based facilities.

6 'Hiding in Plain Sight – Not All That Transmit are Legit', *Windward,* https://windward.ai/content/hiding-in-plain-sight-not-all-that-transmit-are-legit/?submissionGuid=2182472c-8833-4c59-b4eb-1f36adce0ae7, accessed 6 September 2024

7 For example, in January 2024, Sri Lankan authorities used the Sri Lankan vessel monitoring system donated by Australia to help Seychelles Coast Guard interdict a Sri Lankan fishing boat that had been hijacked by Somali pirates. See Bharatha Mallawarachi, 'Seychelles Forces Rescue 6 Sri Lankan Fishermen from Boat Hijacked by Somali Pirates,' *The Washington Times*, 29 January 2024. https://www.washingtontimes.com/news/2024/jan/29/seychelles-forces-rescue-six-sri-lankan-fishermen-/, accessed 6 September 2024

8 For a more complete typology of sensors, see National System for Geospatial Intelligence, *Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1.0,* April 2018. https://www.nga.mil/resources/GEOINT_Basic_Doctrine_Publication_10_.html, accessed 6 September 2024

9 Wim Zwijnenburg, 'On Slicks and Satellites: An Open Source Guide to Marine Oil Spill Detection', *Bellingcat*, 30 August 2024. https://www.bellingcat.com/resources/how-tos/2024/08/30/marine-oil-spill-detection-guide/, accessed 6 September 2024

10 See Robert Cornall and Rufus Black, *2011 Independent Review of the Intelligence Community,* (Australia, Australian Government 2011). p.5. https://www.pmc.gov.au/sites/default/files/resource/download/2011-iric-report.pdf, accessed 6 September 2024

11 Patrick F. Walsh and Mark Harrison, 'Strategic intelligence practice in the Australian intelligence community: evolution, constraints and progress', *Intelligence and National Security*, Vol. 36 No. 5 (April 2021), pp.660-675.

12 Hoang Do, 'Popular MDA Initiatives and Implications for ASEAN' *APCSS Perspectives*, 2 February 2024. https://dkiapcss.edu/nexus_articles/popular-mda-initiatives-and-implications-for-asean/, accessed 6 September 2024

13 Hu Yuwei, Xiao Yan and Chen Yang, 'GT investigates: US uses IPMDA to stir confrontation in South China Sea, while China seeks blue economy partnerships with ASEAN' *Global Times,* 22 December 2022

14 Now called Maritime Border Command.

15 Dinakar Peri, 'National Maritime Domain Awareness centre to be ready in three years', *The Hindu,* 2 January 2024. https://www.thehindu.com/news/national/national-maritime-domain-awareness-centre-to-be-ready-in-three-years/article67698773.ece, accessed 6 September 2024

16 Nicholas Lim and Chong De Xian, 'Maritime Sense-Making and the Role of Big Data Analytics for Enhancing Maritime Security', Pointer, September 2020.

17 Peter Chalk, 'Augmenting maritime domain awareness in Southeast Asia: Boosting national capabilities in the Philippines, Thailand and Indonesia', ASPI Special Report, December 2019. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-12/SR%20150%20Maritime%20domain%20awareness_0.pdf, accessed 6 September 2024

18 Zaeem Hassan Mehmood, 'Pakistan's Maritime Domain Awareness Initiatives in the Indian Ocean, The MOC' Center for Maritime Strategy, 2 July 2024. https://centerformaritimestrategy.org/publications/pakistans-maritime-domain-awareness-initiatives-in-the-indian-ocean/, accessed 6 September 2024

19 https://ifccolombo.org/index.php?id=2, accessed 6 September 2024

20 Most countries also maintain maritime and aeronautical rescue coordination centres to coordinate maritime and air search and rescue operations. They often deal with very similar information as the national information fusion centres in terms of location of vessels and aircraft, but are required by IMO and ICAO regulations to be operated as separate institutions.

21 For example, arrangements between Australia and Indonesia in respect of illegal fishing. See Aristyo Rizka Darmawan, 'Sustainable catch: better Indonesia-Australia cooperation on fishing' *The Interpreter,* 10 October 2022. https://www.lowyinstitute.org/the-interpreter/sustainable-catch-better-indonesia-australia-cooperation-fishing, accessed 6 September 2024

22 They include Comoros, Djibouti, France, Kenya, Mauritius, Madagascar and Seychelles

23 https://www.maxar.com/maxar-intelligence/products/sar-imagery, accessed 6 September 2024

24 Theresa Hitchens, 'NOAA eases licensing restrictions on commercial remote sensing', *Breaking Defense,* 9 August 2023. https://breakingdefense.com/2023/08/noaa-eases-licensing-restrictions-on-commercial-remote-sensing/, accessed 6 September 2024

25 See, *Policies for Maritime Domain Awareness and Space Technology*, The Maureen and Mike Mansfield Foundation, October 2023. https://mansfieldfdn.org/blog/policy-recommendations-for-maritime-domain-awareness-and-space-technology/, accessed 6 September 2024

26 See Global Fishing Watch, 'Our Technology,' https://globalfishingwatch.org/our-technology/, accessed 6 September 2024

27 Siôn Geschwindt, 'This tiny autonomous sailboat is charting a new course for marine science', *Thenextweb,* 5 July 2024. https://thenextweb.com/news/little-autonomous-sailboat-robot-oshen-marine-science, accessed 6 September 2024

28 Heather Mongilio, 'Navy Blocks Iranian Attempt to Steal U.S. Surface Drone in Persian Gulf', *USNI News*, 30 August 2022. https://news.usni.org/2022/08/30/video-navy-blocks-iranian-attempt-to-steal-u-s-surface-drone-in-persian-gulf, accessed 6 September 2024

29 'Task Force 59 Launches New Unmanned Task Group 59.1', US Navy, 16 January 2024. https://www.navy.mil/Press-Office/News-Stories/Article/3645647/task-force-59-launches-new-unmanned-task-group-591/, accessed 6 September 2024

30 'ITU/WMO/UNESCO/ IOC Joint Task Force,' International Telecommunication Union [ITU], https://www.itu.int/en/ITU-T/climatechange/task-force-sc/Pages/default.aspx, accessed 6 September 2024

31 Paul Voosen, ''Smart' fiber-optic cables on the sea floor will detect earthquakes, tsunamis, and global warming', *Science,* 13 March 2024. https://www.science.org/content/article/smart-fiber-optic-cables-sea-floor-will-detect-earthquakes-tsunamis-and-global-warming, accessed 6 September 2024

32 'Norwegian cable network of undersea sensors able to detect submarines found disabled after cables were cut', *Miliary Aerospace,* 22 November 2021. https://www.militaryaerospace.com/sensors/article/14214351/under-sea-sensors-submarines, accessed 6 September 2024

33 'Fact Sheet: Quad Leaders' Tokyo Summit 2022', The White House, 23 May 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/, accessed 6 September 2024

34 'Quad Foreign Ministers' Meeting Joint Statement, Tokyo', 29 July 2024. https://www.foreignminister.gov.au/minister/penny-wong/media-release/quad-foreign-ministers-meeting-joint-statement-tokyo, accessed 6 September 2024

35 See Appendix 1 – SeaVision-IORIS Non-Paper.

36 'Fisheries intelligence, analysis & capacity building to combat illegal fishing,' TMT, https://www.tm-tracking.org, accessed 6 September 2024

37 'Our Story,' International MCS Network, https://imcsnet.org, accessed 6 September 2024

38 'C4AADS is a Nonprofit Organisation with a Mission to Defeat the Illicit Networks that Threaten Global Peace and Security,' C4ADS, https://c4ads.org, accessed 6 September 2024

39 'Decision Support Platform to Accelerate Global Trade,' Windward, https://windward.ai, accessed 6 September 2024

40 'Monitor Your National Waters and Help Protect the World's Oceans,' Starboard Maritime Intelligence,' https://starboard.nz, accessed 6 September 2024

41 Ben Scott, *Adapting Australian Intelligence to the Information Age,* ANU National Security College, 2023. https://nsc.anu.edu.au/sites/default/files/2024-05/Ben%20Scott_AUSINT_WEB_NSC.pdf, accessed 6 September 2024

42 David Brewster and Anthony Bergin, *Australia-India Indo-Pacific Oceans Initiative: Regional Collaborative Arrangements in Marine Ecology in the Indo Pacific Baseline Study,* May 2022. https://ad-aspi.s3.ap-south-east-2.amazonaws.com/2022-07/IPOI%20Report%20-%20Regional%20Cooperative%20Arrangements%20in%20Marine%20Ecology%20-%20May%202022.pdf?VersionId=lihsc6FcmxfJ5yX6soxPuZ3hpOmCxKzz (with Anthony Bergin)

43 'Hawkeye 360 Working With the Pacific Islands Forum Fisheries Agency for Greater Maritime Visibility in the Pacific Islands', 6 July 2023. https://www.he360.com/hawkeye-360-working-with-the-pacific-islands-forum-fisheries-agency-for-greater-maritime-visibility-in-the-pacific-islands, accessed 6 September 2024

44 David Brewster and Anthony Bergin, *Good Neighbours: Strengthening Environmental Security in the Indian Ocean region*, National Security College, February 2023. https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2023-04/web_good_neighbours-strengthening_environmental_security_in_the_indian_ocean_region_v1.pdf, accessed 6 September 2024

45 See generally, David Brewster, *The Pacific Fusion Centre: the challenge of sharing information and intelligence in the Pacific,* Australian Strategic Policy Institute, September 2021. https://www.aspi.org.au/report/pacific-fusion-centre-challenge-sharing-information-and-intelligence-pacific, accessed 6 September 2024. It should be noted that the Pacific Fusion Centre's strategic assessments on Pacific security issues are not publicly available.

46 Ben Scott, *Adapting Australian Intelligence to the Information Age,* ANU National Security College, 2023. https://nsc.anu.edu.au/sites/default/files/2024-05/Ben%20Scott_AUSINT_WEB_NSC.pdf, accessed 6 September 2024

47 Jeffrey Payne, 'Do Not Jettison Traditional Data Sharing in the Maritime Domain', Institute for Security and Development Policy, 11 April 2024. https://www.isdp.eu/do-not-jettison-traditional-data-sharing-in-maritime-domain, accessed 6 September 2024

48 'Evaluation of the Indigenous Ranger Biosecurity Program,' Department of Agriculture, Fisheries and Forestry, December 2022. https://www.agriculture.gov.au/sites/default/files/documents/Evaluation%20-%20Final%20Report%202022%20-%20Indigenous%20Ranger%20Biosecurity%20Program.pdf, accessed 6 September 2024

49 'Indigenous lessons for border force', *The Australian,* 19 February 2024.

50 See *Policies for Maritime Domain Awareness and Space Technology*, The Maureen and Mike Mansfield Foundation, October 2023. https://mansfieldfdn.org/blog/policy-recommendations-for-maritime-domain-awareness-and-space-technology, accessed 6 September 2024

51 Hu Yuwei, Xiao Yan and Chen Yang, 'GT investigates: US uses IPMDA to stir confrontation in South China Sea, while China seeks blue economy partnerships with ASEAN' *Global Times,* 22 December 2022. https://www.globaltimes.cn/page/202212/1282448.shtml, accessed 6 September 2024

Australian National University | NATIONAL SECURITY COLLEGE

Contact

national.security.college@anu.edu.au

nsc.anu.edu.au

@NSC_ANU

National Security College

CRICOS Provider #00120C

TEQSA Provider ID: PRV12002

(Australian University)