JOURNAL OF THE INDIAN OCEAN REGION
2018, VOL. 14, NO. 3, 296–314
https://doi.org/10.1080/19480881.2018.1517437

Give light, and the darkness will disappear:[*] Australia's quest for maritime domain awareness in the Indian Ocean

David Brewster

National Security College, Australian National University, Canberra, Australia

ABSTRACT

There is a growing understanding among maritime security practitioners of the importance of Maritime Domain Awareness (MDA) as an essential enabler of maritime security. This article describes Australia's efforts to develop an integrated national MDA system that brings together data and intelligence from a range of military and civil agencies and commercial sources to which a risk-based assessment is applied. This has become an essential tool to combat transnational maritime security threats in the Indian Ocean and elsewhere. But inherent limitations of national MDA systems are also pushing Australia and other countries to cooperate in trying to improve MDA. This paper then examines ways in which Australia can promote MDA cooperation in the Indian Ocean. It considers the effectiveness and limitations of current and proposed multilateral information sharing arrangements in the region. It concludes that Australia should primarily focus on working with selected Indian Ocean partners to enhance information sharing and help develop integrated national MDA systems.

ARTICLE HISTORY
Received 11 June 2018
Accepted 27 August 2018

KEYWORDS
Maritime domain awareness; maritime security; Indian Ocean; Australian foreign policy; multilateral cooperation

Introduction

On 8 March 2014, Malaysian Airlines flight MH370 and its 239 passengers and crew disappeared without trace somewhere in the Indian Ocean. After fading from radar screens off the northern tip of Sumatra there were no further definitive sightings of the aircraft. The plane seems to have vanished into the vacant southeast Indian Ocean, apparently somewhere in Australia's vast Search and Rescue Region. Despite Australia leading the most extensive search and rescue effort in the world's history involving aircraft and ships from at least 26 countries, the missing airliner has not been found. This tragic incident underlines how huge the Indian Ocean is and how little we really know about what goes on there.

This article discusses Australia's quest for greater maritime domain awareness in the Indian Ocean, principally in relation to civil maritime security threats. The first part sets out some basic concepts in maritime domain awareness (MDA) and why it has come to be seen as an essential enabler for maritime security and governance. The second part of this article summarizes the security challenges that Australia faces in the Indian

CONTACT David Brewster ✉ dhbrewster@bigpond.com

[*] Desiderius Erasmus (1466–1536), Dutch humanist and theologian.

Ocean. The article then discusses Australia's efforts to build a comprehensive and integrated national MDA system that is intended to provide whole-of-government maritime domain awareness of Australia's maritime spaces. While this has been quite successful, national systems will always be limited in their scope and geographic reach. For this reason, Australia and other countries in the Indian Ocean have become increasingly interested in finding ways to share data and intelligence on the maritime domain. The fourth part of this paper discusses Australia's options in enhancing MDA in the Indian Ocean through information sharing arrangements as well as other ways to enhance MDA capabilities.

Australia has much to gain from regional MDA cooperation. Bilateral and multilateral. collaboration through information sharing and capability building can effectively extend the scope and reach of Australia's MDA system as well as improving the effectiveness of national MDA systems of Australia's partners. This article concludes that while multilateral information sharing arrangements might have some limited value, Australia should primarily focus on building a series of bilateral arrangements with particular focus on trusted partners that involves both capacity enhancement and information sharing.

Maritime domain awareness: some basic concepts

The importance of MDA for maritime security

Since the turn of this century there has been a growing realization among security practioners of the importance of MDA as an essential enabler of maritime security. Of course, understanding the position and likely intention of maritime actors has always been a major concern of navies. But only with recent advances in sensor and computing technology has it become possible, at least in theory, to create a networked real time picture that allows for a shared understanding of threats and developments in the maritime domain. It is no longer sensible or sufficient to invest in platforms and sensors to collect information without also creating a system for aggregating, analysing and disseminating that information (Biddington, 2014, 6).

In 2005, the United States launched a national MDA project called the *National Plan to achieve Maritime Domain Awareness* as part of its Maritime Strategy for Homeland Security. Over the last decade or so, MDA has come to be understood as a key component of US navy's maritime strategy. Technological development means that the level of MDA that can now be achieved is of a different order than ever before. During the Cold War the United States tracked probably less than 1,000 ships worldwide at any given time. That number is now in the hundreds of thousands, with links to cargoes, crews and financial transactions (Boraz, 2009). The ultimate intent of that project was to be able to track the entire global merchant fleet, which consisted of approximately 90,000 ships in 2016 (Equasis, 2016). In the words of the US Navy's Director of Naval Intelligence: 'As we evolve down the road we'll get closer to tracking all [merchant ships] that are in the world on a minute-by-minute basis' (Munns, 2005; Rahman, 2008).

In undertaking its national MDA project, the United States has recognized that even with its massive defence resources and global network of defence assets it could never achieve MDA alone and that achieving global and even regional MDA would be highly dependent upon multilateral cooperation.[1] This was an important factor behind the USsponsored *Global Maritime Partnership Initiative* (sometimes called the '1000-ship Navy'), announced in 2005, under which the US Navy sought to encourage navies throughout the world to develop networks to counter transnational maritime security challenges. Although that particular initiative now receives relatively little attention, the imperatives behind it still drives the need to build international networks.

What is maritime domain awareness?

There are various definitions of MDA, although in broad terms they all involve gaining an understanding of the position and intention of actors in a given maritime environment.[2] The Australian Government defines *maritime domain awareness* as 'The effective understanding of anything associated with the *maritime domain* that could impact the security, safety, economy, or environment.' For these purposes, the *maritime domain* is defined by the Australian Government as 'all things relevant to the national interests on, under, associated with, or adjacent to Australia's maritime zones.'[3]

The Australian definition of *maritime domain awareness* generally follows the definition used in the US National Maritime Domain Awareness Plan (US Government, 2005). But in light of its global responsibilities the United States employs a broader, more functional, definition of the *maritime domain* as: 'All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances' (US Government, 2004). In practice, despite official definitions, the geographic scope of Australia's MDA activities extend far beyond its Exclusive Economic Zone (EEZ).

The quest for better situational awareness is not confined to the maritime domain, but is also occurring in other domains such as land, air and space. But in comparison with these other domains, there are additional complications in the maritime realm. One is that the maritime domain is multidimensional – we not only need an understanding of what is happening on the surface of the water, but also below the surface and in the air above. A second complication is the intersection of a plethora of commercial, government and international interests that commonly occur in the maritime domain that do not occur to the same extent in, say, the land domain. Thus the maritime domain experiences complex cooperative and competitive interactions of multiple actors that are also often subject to (complex) rules of international law, located in areas that may or may not be the subject of maritime territorial disputes (Biddington, 2014, 14).

Civil maritime domain management and MDA

As noted, this article focusses on MDA in connection with civil maritime security threats faced by Australia in the Indian Ocean. As a starting point, one can conceptualize the overall task of *civil maritime domain management* as comprising three interconnecting parts that together provide effective management of the maritime environment. These are:

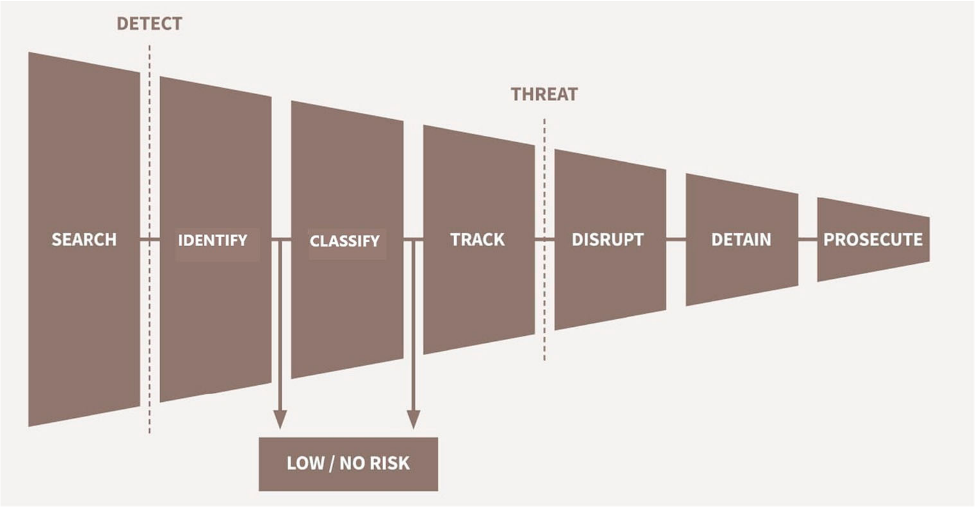
- *Maritime Domain Influence* – the ability to influence the maritime domain through policies that influence relations with domestic and international partners.
- *Maritime Domain Awareness* – discussed in this paper.

- *Maritime Domain Response* – broadly, the ability to respond to identified threats.

Thus, within the overall ambit of civil maritime domain management, maritime domain awareness provides a vital link between a country's ability to *influence* its maritime environment and its ability to *respond* to threats.

One can think about MDA systems in different ways. One way is that it is a complex *system of systems* that must all work together. These component systems include collection of information and data, including through reconnaissance, surveillance and reporting; aggregation of data in a central location; analysis/processing – the interpretation of information involving tools such as visualization of information and statistics and trends analysis; and dissemination that involves the distribution of results to decision-makers and users. These component systems will be discussed in some detail later in relation to MDA systems in general, and Australia's MDA system in particular.

Another way of looking at an MDA system is that it is a set of *procedures* through which awareness can be achieved and then used to respond to threats. An MDA *procedural chain* can be represented as follows:[4]



For these purposes:

- *Searching* involves surveying a geographic area using active or passive technical or non-technical means with the aim of identifying anomalous behavior.
- *Detection* is the moment when an object or vessel is discovered through one or more sensors, visual detection or self-reporting through automatic identification systems (AIS).
- *Identifying* the vessel may involve data from a variety of sources.
- *Classifying* the vessel by level of risk, taking into account factors such as location, track, type and whether it is using an AIS.
- Accurate *tracking* enables authorities to determine the vessel's direction and possible destination, which may further elucidate the threat posed. If necessary, it also informs the planning of an interception at sea or on land.

- *Disruption* may involve the arrest and detention of crew members or confiscation of illicit cargo. If the vessel is involved in an illegal activity, the interception/interdiction itself may disrupt that activity.
- Where appropriate, a vessel may be *detained,* and if enough evidence is available to prove that a criminal offence has occurred, offenders may be *prosecuted*.

The common operating picture

The center-piece for MDA systems is the creation of a Common Operating Picture (COP). This is the sum of data and intelligence drawn from many sources and organizations e.g. data from commercially operated Automatic Identification Systems, military or civil radar tracking, or incident reports from law enforcement agencies. This data is then cross-referenced and correlated (or 'fused') into a coherent single picture that is accessible to many users.

An 'awareness' element is then applied to the data to produce a Recognized Maritime Picture, from which a Recognized Threat Picture can be developed.[5] This will involve the assignment of threat levels to each actor on the basis of known information and 'rule sets.' For example, a vessel lacking positive data may be assigned a high threat level by default which is reduced as vessel, crew and cargo criteria are validated from information already collected by various government agencies. Importantly, the efficiency of the system in identifying anomalies (and identifying threats from anomalies) without generating too many false positives will be heavily dependent on the level of understanding of the operating environment embedded within the system. This requires a deep knowledge of the practices and customs of the commercial shipping and fishing industries, which are likely to account for the great majority of vessels in a given maritime domain. For example, when can an unexpected deviation of a vessel from its course be otherwise explained by 'normal' industry factors? The minimization of the number of false positives generated by the system allows human analysts to focus on a smaller number of 'real' threats.

There are many technical challenges in creating a COP drawn from many different sources and agencies, including in synthesizing different data formats, time stamping, data storage and retention, data modification and symbology. Importantly, raw data must be subjected to analysis (both human and computer) to identify anomalies or other matters of interest. This is key to creating what is sometimes called 'shared understandings' (Bueger, 2015).

The COP is intended to help decision-makers to make decisions and take action on the basis of shared, reliable and trustworthy information. It reflects the 'need to share' principle in relation to information that has come into vogue post-911, replacing the previous 'need to know' mantra. The COP is particularly important where cross-organisational coordination is required, which is frequently the case in the maritime domain. The COP can help rule in or rule out possible courses of action and provide the basis for an agreed approach, including the assignment of responsibilities and resources (Biddington, 2014).

One of the biggest challenges in creating a COP is the civil–military-commercial divide. Data on the maritime domain will be sourced from a variety of military, law enforcement and civil government agencies. Commercial entities are also a key source of information on shipping (e.g. from satellites or terrestrial Automatic Identification Systems). Each type of entity will have its own agenda, motivations and concerns about confidentiality/secrecy. This is an obvious issue for military or law enforcement agencies, but can also create significant sensitivities for commercial actors. The location, course, speed and cargo of a particular ship might be of interest to government agencies for various reasons, but they can also be significant commercial secrets that would be of great interest to competitors.

The willingness of agencies to share data and intelligence with other national agencies is therefore a key threshold in creating a COP. Any threat-based assessments will also require the establishment of a *common threat lexicon*, so that various user agencies use the same terms in describing potential threats. The COP also needs to be usable for a variety of military, law enforcement and civil purposes, each with its own particular needs and limitations. Effective MDA systems must simultaneously serve multiple users that have different priorities and time imperatives and they seek information at different levels of detail or granularity (Barnes, 2018). These factors substantially complicate the COP, meaning that it must simultaneously operate on several different levels, including different levels of confidentiality or secrecy.

Challenges of sharing information across national borders

In practice, achieving MDA over a broad area of the maritime domain requires the sharing of information with other countries. Even a superpower such as the United States freely acknowledges that achieving maritime domain awareness across its maritime domain is only possible in conjunction with many partners. For a middle power such as Australia, with a small population and limited resources, but with interests over large areas of the Indian Ocean, not to mention the Pacific and Southern Oceans, MDA can only be achieved across its entire maritime jurisdiction in cooperation with others. This not only includes data that can be shared real time to facilitate coordinated responses, but also non-real time data can be used to identify trends and patterns.

While multinational information sharing may be essential for achieving MDA, the addition of numerous national military and civil agencies into the mix makes establishing a multilateral COP for several different purposes (e.g. monitoring fishing catches, tracking drug smugglers or providing search and rescue services) extremely difficult. Any attempt to share information across borders among civil agencies, law enforcement organizations and quasi-military entities raises many additional legal, political and security issues around maintaining security of data and intelligence and the uses to which information may be put.

Aside from normal national security concerns, there are many other examples of problems that need to be addressed in cross-border information sharing. National agencies may be concerned about maintaining commercial confidentiality in relation to that country's commercial or fishing vessels. Some agencies may, for example, acquire shipping information from commercial providers on terms that it cannot be shared with other countries. In other cases, law enforcement authorities may be unwilling to share information with authorities from other countries that might result in the application of the death penalty to one of their own nationals (as is the case with Australia). Complications such as these that might potentially be resolvable through the negotiation of bilateral protocols or agreements can be magnified almost exponentially when contemplating sharing information on a multilateral basis.

These challenges mean that even the most longstanding and trusted allies, such as the Five Eyes partners, can find it difficult to create a shared picture. The Five Eyes partners have established a Maritime Domain Awareness (FVEYMDA) Working Group, but were only able to implement a shared Vessel of Interest (VOI) Lexicon in 2017 – only a first step towards achieving a shared COP. Top US military officials acknowledge that militaries need to fundamentally rethink information sharing among allies (such as Five Eyes) and other partners so that, for example, 'no foreigner' security classifications become the exception rather than the default position (Pomerleau, 2016).

Australia's civil maritime security challenges in the Indian Ocean

The Indian Ocean is one of the largest bodies of water in the world. Its vast size and emptiness, and the relative lack of resources of most littoral states, has also made it is one of the least governed spaces on the planet (Bateman, 2016). Achieving maritime domain awareness there will be an essential starting point for addressing the myriad of maritime security challenges in the Indian Ocean and establishing a system of governance of that space through national agencies and in cooperation with the agencies of other countries.

For Australia, an island-continent-nation with a population of some 25 million people, proper governance of the Indian Ocean represents a major national challenge. Australia has by far the largest Indian Ocean coastline and by far the largest area of maritime jurisdiction of any Indian Ocean state. According to international definitions, the Indian Ocean coastline of the Australian continent is longer than 14,000 km. Australia has a maritime jurisdiction in the Indian Ocean of around 5.9 million square km, including an EEZ of 3.88 million square km and an extended continental shelf of 2.02 million square km (Bateman & Bergin, 2010). Australia's official search and rescue zone and so-called Security Forces Authority Area encompasses most of the eastern half of the ocean. Australia's security interests extend as far as the western Indian Ocean and Persian Gulf, where the Royal Australian Navy has been deployed virtually continuously since 1990. Together with Australia's areas of interest in the Pacific and Southern Oceans, Australia's maritime security interests cover a considerable portion of the earth's surface.

The geography of the Indian Ocean also contributes to Australia's challenges. It is a 'concave' space with few islands and huge distances between land. The distances and relative lack of cooperation among littoral states makes it a virtual 'black hole', creating some unique challenges for Australia in providing security in this maritime space. But the geography of the Indian Ocean can also help in some respects. The existence of a handful of maritime 'chokepoints' (such as Malacca Strait, Sunda Strait, Lombok Strait, Strait of Hormuz and Bab-el-Mandab) through which most large vessels entering and exiting the Indian Ocean must pass can also allow resources to be focused on these areas (Biddington, 2014, 23).

The Australian Government's *Guide to Australian Maritime Security Arrangements* (known as 'GAMSA'), identifies eight key civil maritime security threats faced by Australia in addition to military maritime security threats. These include:

- Irregular maritime arrivals
- Illegal exploitation of natural resources
- Illegal activity in protected areas
- Marine pollution
- Prohibited imports and exports
- Compromise to biosecurity
- Piracy, robbery or violence at sea
- Maritime terrorism

All of these threats are prevalent in the Indian Ocean – in fact, far more so than Australia's other maritime domains (the Pacific and Southern Oceans). The Indian Ocean is in many ways an oceanic 'wild west', where maritime security threats presented by criminal and other non-state actors generally far exceed those in other oceans. Although these challenges generally lie at a transnational or sub-strategic level, some have a significant economic and social impact on littoral states, especially those that have a high reliance on maritime economy and resources. Some sub-strategic threats can also rise to a strategic level, such as Somali-based piracy which over the last decade or more presented such a threat to international commercial trade that it elicited a major naval response from countries inside and outside the Indian Ocean region. The nature and extent of transnational maritime security threats in the Indian Ocean and the relatively low level of capabilities of most littoral states has led to a focus on building mechanisms for maritime governance in the Indian Ocean, including mechanisms for better cooperation among regional navies and coast guards (Bateman, 2016).

The transnational security challenges that Australia faces in the Indian Ocean, including people and drug smuggling, illegal fishing, environmental challenges and search and rescue responsibilities, are generally most evident in the western Indian Ocean. However, these challenges also increasingly affecting waters in the eastern Indian Ocean, closer to Australia.

Maritime security threats are also frequently interlinked. A failure to address illegal, unreported and unregulated (IUU) fishing, for example, can allow for the growth of transnational criminal networks that will likely also to be involved in other activities such as people, drugs and arms smuggling (whether or not on the same vessels) (Noonan & Williams, 2016). It is not easy therefore to clearly separate maritime security threats simply by nature or by location.

Since 2001, Australia's principal maritime security focus in the Indian Ocean has been on border protection and particularly so-called 'irregular maritime arrivals' in Australian waters. The threat of irregular maritime arrivals has driven considerable investment in Australia's maritime surveillance and enforcement capabilities over this period. This has included the establishment of the Australian Border Force (ABF) and its Maritime Border Command (MBC) as a quasi-coast guard agency with responsibilities over large parts of the eastern Indian Ocean. The ABF employs a 'whole of government' approach in coordinating civil enforcement with civilian agencies and the Australian Defence Force (ADF), using a combination of assets and resources to fulfill its tasks. Although this model continues to evolve, to date it has been quite successful in achieving its objectives over an extended area of jurisdiction using relatively limited resources. Indeed, over the last decade Australia has developed sophisticated and comprehensive maritime security capabilities covering much of the eastern Indian Ocean, with particular focus on the Australia's northwest approaches. This has allowed the ADF and ABF to successfully conduct maritime barrier operations that have successfully reduced irregular maritime arrivals in Australia to zero between 2015 and August 2018 (Phillips 2017). How long this can be maintained is an open question.[6]

Australia's national MDA system

Australia has probably the most sophisticated national MDA system of any Indian Ocean state. A key element of Australia's MDA system is the Australian Maritime Identification System (AMIS), which was introduced in 2005 and is intended to provide whole-of-government maritime domain awareness across the military and civil domains. It is a multi-level secure ocean surveillance system that brings together all shipping data available to Australian Federal agencies (Asia Pacific Defence Reporter, 2011). This includes defence forces, intelligence agencies, law enforcement and immigration agencies, the Australian Maritime Safety Authority (AMSA) and the Australian Fisheries Management Authority (Rahman, 2010).

AMIS differs from prior systems that were focused on reporting vessels sailing to and from Australian ports, which allowed non-reporting ships through the net. This problem became apparent in the MV *Pong Su* incident in April 2003 when a North Korean registered vessel which was not bound for any Australian port was caught smuggling heroin onto a beach in Victoria on the southeast coast of Australia. It was realized that Australian agencies had all the data to hand to identify, track and apprehend this drug-smuggler well before the vessel reached Victoria, but at that time there was no agency responsible for putting the data together and acting on it (Asia Pacific Defence Reporter, 2011).

Some of the major categories of data and intelligence that feed into the Australian Maritime Identification System include:

- Data from vessels and aircraft operated by the Australian Defence Force. The ADF's key air surveillance platforms include P-8A Poseidon maritime surveillance aircraft, P-3C Orion aircraft (now being retired) and E-7A Wedgetail AEW&C aircraft, all operated by the Royal Australian Air Force. These will be supplemented by MQ-4C Triton unmanned aerial vehicles (UAVs) in coming years.
- Data from vessels and aircraft operated by the Australian Border Force. The ABF operates its own fleet of 8 *Cape* Class OPVs and 2 cutters, as well as 10 *Dash-8* aircraft under contract.
- Data from 5 *Dornier Do328-120* aircraft operated under contract for the Australian Maritime Safety Authority.
- Data from AMSA's Modernized Australian Ship Tracking and Reporting System (MASTREP). This uses an Automatic Identification System (AIS), which is automatically broadcast via VHS and received via satellite and terrestrial stations. It covers Australia's Maritime Search and Rescue region and further afield. AIS must be used by Australian vessels and foreign vessels in Australia's territorial waters other than in the course of innocent passage.[7] The AIS reports every six hours, providing information on the vessel, its position, course and speed as well as safety-related information.[8]
- Data on domestic port movements from AMSA.[9]

- Data from coastal surveillance radars located on mainland Western Australia as well as on Christmas Island (installed in 2013). These have a range of approximately 200 km.
- Data from Australia's long range over-the-horizon radar system, the Jindalee Operational Radar Network (JORN). JORN facilities, which are located in Queensland, Northern Territory and Western Australia, potentially allow the detection of air and surface targets up to 4,000 km away (i.e. beyond Cocos Island) (Styles, 1998). Despite its potentially long reach, the JORN system has several limitations in terms of the limited size of its so-called 'tile' (the specific area that the radar's energy is directed onto), its intermittency and difficulties in detecting small vessels.[10] The JORN system is currently being upgraded (Daigle, 2018).
- Satellite imagery, including through a contract with DigitalGlobe, a commercial provider that maintains five global satellites (Abbey, 2017).
- Limited data from a domestic Vessel Monitoring System (a satellite-based closed polling system) used by some fishing vessels in Queensland waters.
- National and international intelligence, including intelligence from Australia's Five Eyes intelligence partners and through limited bilateral arrangements with regional partners.

In the future, Australia is likely to place increasing reliance on unmanned vehicles for surveillance of the maritime domain, including UAVs such as MQ-4C Tritons which are now being acquired by the RAAF, as well as unmanned maritime vehicles (UMVs) (Mugg, Hawkins, & Coyne, 2016).

The AMIS is operated by the MBC's Australian Maritime Border Operations Centre in Canberra. Its responsibilities include the production of operational and tactical intelligence information regarding vessels operating within Australia's maritime environment and coordination of the MBC's air and sea operations. MBC adopts an intelligence-led, risk-based approach (for example, assessing the risk posed by a vessel depending on its location, its type and whether it is using an AIS) to plan and undertake both strategic maritime surveillance and targeted operations.

A key component of AMIS for the analysis of data is the Australian Maritime Threat Risk Assessment Capability (known as 'AMTRAC'), which supports the wider intelligence-led management strategy. Automated advanced profiling identifies both present and emerging threats along the border continuum (Australian Customs and Border Protection Service, 2014, 22). Potential threats may be based on data including the vessel (all known information pertaining to the vessel); the voyage (crew, cargo and passengers); and the track (behavioral movement). AMTRAC places considerable reliance on using artificial intelligence to do much of the work in identifying anomalies from the normal operating environment. Once a threat is detected then it must be validated by a 'human in the loop' before it is forwarded to the appropriate agency. False positives are used to 'teach' the AI system.

It has been claimed that the AMIS has been 'exceptionally successful' in terms of bringing together data and intelligence available to Australian military and civil agencies (Asia Pacific Defence Reporter, 2011).[11] Despite its success, without enhanced regional cooperation, the AMIS will have inherent limitations in scope and geographic reach in achieving MDA across the Indian Ocean.

Approaches to regional cooperation in building MDA in the Indian Ocean

Australia has two basic objectives for promoting MDA cooperation in the Indian Ocean. The first, as noted above, is to effectively extend the scope and reach of Australia's MDA system through gaining access to data or intelligence from partners. This may allow the early detection of vessels of interest and the provision of confirmation on vessel and personnel locations. The second objective, of no less importance, is to help enhance the MDA capabilities of Australia's Indian Ocean partners in order to strengthen their own maritime security efforts. Both these objectives can be pursued through a combination of information sharing and capability enhancement.

The Australian government has repeatedly indicated that strengthening regional MDA cooperation should have priority in Australia's regional strategy. Australia's *2016 Defence White Paper* pledged that: 'we will work with regional partners to develop shared maritime domain awareness capabilities that provide a basis for greater maritime security cooperation' (Department of Defence, 2016, para 5.47). Australia's *2017 Foreign Policy White Paper* was even more explicit on the need to expand regional MDA cooperation, stating:

> Australia will increase its investments in maritime security capacity building in Southeast Asia. We will also work to strengthen the focus on maritime issues within regional forums, including the EAS [East Asia Summit] and IORA [Indian Ocean Rim Association], and enhance regional training on maritime domain awareness, protection of the marine environment and international law. We will deepen joint exercises and build maritime domain awareness with India and collaborate on maritime safety and security with other Indian Ocean partners, like Sri Lanka (Australian Government, 2017, 47).

But despite the imperative language of these policy statements, there has been relatively little implementation of these policy statements in practice in the Indian Ocean.

Regional information sharing arrangements

There are some bilateral and multilateral information sharing arrangements in Southeast Asia (in which Australia is involved), and some nominal arrangements in the western Indian Ocean (in which Australia does not directly participate). But there are no established pan-Indian Ocean multilateral information sharing arrangements. There are also few bilateral arrangements which would assist Australian authorities in tracking threats emanating from beyond the reach of its national MDA system. What are Australia's options in developing regional information sharing arrangements in the Indian Ocean?

Multilateral information sharing arrangements

There are several existing MDA information sharing arrangements in Southeast Asia, including three multilateral information sharing or fusion centers in which Australia participates. Two of these arrangements, the Information Sharing Centre (ISC) of the Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia (ReCAAP);[12] and the Piracy Reporting Centre (PRC) of the International Maritime Bureau[13] are both focused on *post facto* reporting and analysis of incidents of piracy and armed robbery at sea in and around Southeast Asia. This data can be of some analytical use, although its non-real time nature limits its actionable value.

The Information Fusion Centre (IFC) operated by the Singapore Navy takes a broader multi-issue maritime security approach and is intended to provide real time actionable intelligence on threats.[14] The Singapore IFC has institutionalized linkages for information sharing with over 78 agencies in 38 countries. As at 2017, Liaison Officers from around 16 countries (including Australia) were co-located in the IFC's Maritime Security Centre. Information received by the Singapore IFC is fused into its Open and Analysed Shipping Information System (OASIS) which is also integrated into the Western Pacific Naval Symposium Regional Maritime Information Exchange and Malacca Straits Patrols' information System. But while the Singapore IFC is the most sophisticated multilateral arrangement in Southeast Asia, the system suffers from constraints in its threat detection capabilities. Bueger notes that the IFC may be better suited for incidence response rather than early threat detection, and the center has also been subject to recent budget cuts by the Singapore government, which may further limit its effectiveness.[15]

According to Bueger, the multilateral MDA arrangements in Southeast Asia provide a flexible and adaptable regional MDA structure and a role model for MDA systems elsewhere (Bueger, 2015). Whether or not that may be the case in the long term, this article argues that for Australia the practical value of these systems in the Indian Ocean (that is, beyond the immediate waters of the Southeast Asian archipelago) will likely be limited for many years to come. As discussed below, Australia may achieve better outcomes from focusing its limited resources on building regional MDA capabilities in the Indian Ocean through bilateral cooperation.

Several maritime information-sharing or fusion centers have also been established in the western Indian Ocean, which Australia does not participate in directly. Most MDA in the western Indian Ocean is provided by extra-regional actors rather than regional states, including the European Union's Naval Force Atalanta (EUNAVFOR Atalanta) and its Maritime Security Centre Horn of Africa (MSCHoA). According to Bueger, as of 2017 the MSCHoA was the backbone of the MDA system in the region (Bueger, 2017, p. 2). The MSCHoA's Mercury information sharing system provide a technical mechanism for the sharing of information and coordination of operations. The European Union has also taken a leading role in the establishment of information sharing centers at Antananarivo in Madagascar (which uses the Singapore IFC as its template) and has also supported centers established under the Djibouti Code of Conduct in Yemen, Kenya and Tanzania. The achievements of these projects remain limited and as at 2017 the region is a long way from having an independent MDA structure. According to Bueger, thus far the centers have not enabled the sharing of information, conduct research and analysis of maritime developments, provide a shared maritime picture and coordinate operations. They are hampered by a lack of trust and confidence and there is no willingness to share information with the centres (Bueger, 2017, p. 2). Importantly, for the foreseeable future, none of these arrangements appear capable of providing much actionable information relevant to Australia's primary area of interest in the eastern Indian Ocean.

There might also be lessons from the multilateral information sharing arrangements that are gradually evolving in the South Pacific. These are developing in a decentralized manner and operate at several functional levels. For a start, Australia's Pacific Maritime Security Program[16] and the associated Operation *Solania* air surveillance program (led by Australia, France, New Zealand and the United States), provide valuable data inputs for host countries as well as Australia's national MDA system (Department of Defence, u.d.). There are also separate functional information sharing agreements among national agencies, including Australian agencies, relating to fisheries (the Pacific Islands Forum Fishing Agency, which operates the FFA Regional Fisheries Surveillance Centre in Honiara), law enforcement (Pacific Transnational Crime Network, which operates the Pacific Transnational Crime Coordination Centre in Samoa), customs (Oceania Customs Organisation) and immigration (Pacific Immigration Directors' Conference). These information sharing arrangements do not (yet) feed into a single regional COP.

However, in September 2018, the Australian Government announced that it would work with Pacific governments to establish a 'Pacific Fusion Centre' that would help decision-makers to respond to threats such as illegal fishing, people smuggling and narcotics trafficking. It is hoped that this initiative will build incrementally on existing information sharing arrangements. Anthony Bergin and Christian Bueger stress that in developing the MDA architecture in the South Pacific, the region needs to take an incremental approach that pursues realistic goals and ensures ownership and sustainability. Any architecture shouldn't focus just on threats or crime. It should also ensure that measures benefit the larger blue economy and regional ocean governance (Bueger & Bergin, 2018).

The South Pacific may provide important lessons for cooperation in the Indian Ocean. One lesson comes from the success of Australia's Pacific Maritime Security Program in promoting national MDA capabilities of smaller countries. The potential application of a capacity building program of this nature to the Indian Ocean is discussed below. A second lesson may be to focus, at least initially, on developing information sharing arrangements between counterpart national law enforcement agencies rather than on immediately aspiring towards a multilateral all-purpose MDA center. While sharing between counterpart agencies is seemingly practical and incremental, it should be remembered that even this approach will be constrained by the lack of a history of cooperation among Indian Ocean countries as compared with the South Pacific. This might suggest that Australia should promote enhanced information sharing arrangements among enforcement agencies from selected eastern Indian Ocean countries (such as India and Indonesia), which could potentially then be extended to others at a later time.

Bilateral information sharing arrangements

Australia already has some bilateral information-sharing arrangements with selected Indian Ocean partners for specific purposes, reflecting their particular shared interests. Australia has longstanding defence relationships with Singapore and Malaysia, including as part of the Five Power Defence Arrangement, which include sharing of naval information in Southeast Asia.[17] For several years, Australia and Sri Lanka have also exchanged information on suspected people smuggling vessels. This arrangement has proved very useful in helping to deter or interdict people smuggling vessels originating in Sri Lanka.

In early 2018, the ABF and its Indonesian counterpart, the Indonesian Maritime Security Agency (BAKAMLA) signed an information sharing agreement relating to IUU fishing, which is an outcome of the Australia-Indonesia Joint Maritime Declaration which was signed in February 2017 (Australian Border Force, 2018). The arrangement is still to be fully operationalized and will likely involve information sharing on suspected IUU fishing vessels on a case by case basis.

One bilateral arrangement of potential significance is the so-called 'white shipping' information sharing agreement between Australia and India, operationalized in 2017.

India has placed much greater emphasis on MDA efforts following the maritime-based terrorist attacks against Mumbai in November 2008 (Baruah, 2018). This led to the establishment of the Information Management and Analysis Centre (IMAC) as the center point of an Indian national MDA system. Since 2014, India has pursued 'White Shipping Agreements' for exchange of white shipping information on the identity and movement of commercial non-military vessels with government agencies of 26 countries and 3 multinational groups (Government of India, 2016). As at late 2017, India had signed or were in the process of negotiation of agreements with Australia, France, Israel, Singapore, Thailand, the United States, Vietnam, Sri Lanka, Myanmar, Kenya, Bangladesh, Indonesia, Maldives, Malaysia, Mauritius, Myanmar, Seychelles, Sri Lanka, Thailand and Italy (Basu, 2017; Business Daily Africa, 2017; Sputnick, 2017). These are strictly bilateral arrangements although India's partners access it through a common platform operated by India. But India's partners do not have access to a COP, and there is no sharing of data with other partners without agreement.

At the IORA Summit in Jakarta in 2017, India proposed the establishment of a regional MDA hub, based in India, under the auspices of the Indian Ocean Rim Association. It appears that Delhi contemplates evolving bilateral information sharing arrangements (where India acts a hub) into a multilateral arrangement. Indian analyst, Shishir Upahyaya, advocates establishing a pan-Indian Ocean system using the European Maritime Safety Authority (EMSA) as a model (Upadhyaya, 2017). While such an arrangement may be useful, it would also carry limitations which may become more evident as the number of national participants in the system grows.

Enhancing regional capabilities

Another important – and perhaps most important – way of enhancing regional MDA is to focus on enhancing national capabilities of selected Indian Ocean partners. This may involve assisting partners to acquire or develop platforms, sensors and MDA systems. Australia's successful Pacific Maritime Security Program (formerly the Pacific Patrol Boat program) in the South Pacific has already been noted. Australia's most successful experience in the Indian Ocean involved the giving of two surplus *Bay* class patrol boats to Sri Lanka in 2013, principally driven by Australian concerns about people smuggling activities originating in Sri Lanka. These platforms formed an important basis for a broader security partnership that has developed since that time which includes information sharing on people smuggling and various other transnational criminal activities. This relationship has been successful in enhancing maritime domain awareness for both Sri Lanka and Australia.

There is considerable scope for Australia to develop similar bilateral partnerships with countries such as Bangladesh, Myanmar and Indonesia in the crucial eastern Indian Ocean area, involving a combination of capability enhancement and information sharing in the context of transnational maritime law enforcement (Brewster, 2018). Australia has particular expertise to offer in assisting regional partners to develop integrated national MDA systems that bring together information that may already be available to various government agencies.[18] Importantly, partnerships to help develop MDA capabilities of developing countries should as much as possible focus on low-tech rather than high-tech solutions, including collating public information and working with coastal populations and greater coordination between maritime-security related projects (Bueger, 2017).

There is also consideration scope for cooperation with more capable Indian Ocean partners, for example, through the sharing of facilities. Australia has much to offer partners such as India and France, including valuable air staging facilities at Cocos Island (Brewster & Medcalf, 2017) and at Darwin on the Australian mainland which are located close to transit points through the Indonesian archipelago such as the Sunda and Lombok straits. Such arrangements could also involve Australia gaining access to facilities operated by its partners.

Conclusion

Where does all this lead Australia in its quest for maritime domain awareness in the Indian Ocean? Since the turn of this century there has been growing recognition throughout the world that maritime domain awareness is an essential requirement for maritime security and governance. While MDA systems are primarily national-based (and will continue to be so for the foreseeable future), they also require significant international cooperation to transcend the inherent limitations of national systems.

The Indian Ocean is a vast, largely ungoverned, maritime space in which Australia has crucial interests. It is the location of numerous transnational maritime security challenges, including piracy, IUU fishing, smuggling of people, arms and drugs and threats presented by natural disasters and climate change. These threats are frequently interlinked, so that failure to address one will facilitate the growth of other threats. In the past, many of these problems have been more prevalent in the western Indian Ocean than in the eastern Indian Ocean, but this may be changing.

Over the last decade, Australia has been relatively successful in addressing maritime security issues such as people smuggling in its waters, and its national MDA system has been a key enabler of this. However, there are indications that many of security challenges prevalent in the western Indian Ocean are moving eastwards into waters closer to Australia. This will likely include new threats from people smuggling as past push factors move to different parts of the Indian Ocean region (e.g. driven by civil conflicts or climate change).

Australia has been relatively successful in building an advanced national MDA system that applies a whole-of-government approach in bringing together data and intelligence available to Australian military and civil agencies. But this will always be subject to limitations in scope and geographic reach which can only be overcome through international cooperation. For this reason, Australian strategic statements make clear that building regional cooperation in MDA is a national priority.

Australia has two basic objectives for promoting regional MDA cooperation in the Indian Ocean. The first is to effectively extend the scope and reach of Australia's MDA system. The second is to enhance the MDA capabilities of Australia's Indian Ocean partners in order to strengthen their own maritime security efforts. Both these objectives can be pursued through a combination of information sharing and capability enhancement.

While multilateral MDA systems can be very useful in theory, their practical value can be limited by their multilateral nature which will often inhibits information sharing. Despite these limitations, Australia should nevertheless support India's efforts, under the auspices of IORA, to incrementally develop a multilateral pan-Indian Ocean information sharing arrangement.

Australia's experience in the South Pacific, where multilateral information sharing arrangements were built incrementally between various counterpart agencies (e.g. fishing, immigration, customs, policy) prior to the development of a fusion centre may be a useful model to promote multilateral information sharing in the Indian Ocean. However, this approach may also be constrained by the historical lack of cooperation among Indian Ocean countries, as compared with the South Pacific.

Australia should draw from its successful experience with Sri Lanka to enhance MDA cooperation with eastern Indian Ocean countries such as Bangladesh, Myanmar and Indonesia. Mutual information sharing arrangements can be useful, but for the moment, building national capabilities may be more important. Australia could, for example, potentially play an important role in advising those countries on the development of integrated national MDA systems that bring together existing sources of information.

In promoting regional MDA cooperation, Australia needs to focus on cooperative MDA arrangements with key Indian Ocean partners such as India, Indonesia, France and Sri Lanka. Limited information sharing with certain trusted partners could eventually be expanded into sharing of information on grey shipping and, potentially, the sharing of assets and facilities.

Notes

1. The concept of MDA inherently involves a spectrum of awareness, ranging from non-awareness to absolute awareness. While absolute awareness of everything present or occurring within a given maritime domain (and the intention of each actor) might be an aim, it is not realistically achievable. Accordingly, when this article discusses 'achieving MDA', it means achieving a sufficient level of MDA for a given purpose. Thus, 'achieving MDA' for the purposes of enforcing fishing regulation will require a different type of awareness compared with say achieving MDA in respect of certain military threats.
2. The phrase 'maritime situational awareness' is sometimes used as an alternative to maritime domain awareness, although MDA may be somewhat wider in concept in including maritime intelligence (Bueger, 2015, 159).
3. Australian Government (2013). The *Guide to Australian Maritime Security Arrangements* further notes that threats to security may arise from outside Australia's maritime jurisdiction due to geopolitical, environmental, and resource issues in Australia's region and that consequently, management of the threats to Australia's security at times will require consideration of areas beyond the EEZ. The Royal Australian Navy uses a similar definition of MDA, although it defines *maritime domain* somewhat more narrowly as: 'The series of jurisdictional zones that surrounds the coast of a State. It includes territorial seas and the EEZ.' (Royal Australian Navy, 2010, p. 199). This is currently under review.
4. Adapted from Mugg et al. (2016, pp. 7–8).
5. This paper will collectively refer to these using the broad and widely-used term 'Common Operating Picture.'
6. The unexpected arrival of 17 Vietnamese asylum-seekers in for north Queensland on Australian's Pacific Coast, in August 2018, was the cause of considerable embarrassment for Australian authorities.
7. MASTREP has been in operation since 2013, replacing the previous AUSREP system, which was a passive polling system operated by INMARSAT.
8. AMSA also receives similar data from its Long Range Identification and Tracking (LRIT) system. This is a satellite-based polling system mandated by the IMO for international voyaging ships

of more than 300 gross tonnage and all passenger ships regardless of size. LRIT data includes positional, timing and merchant shipping identity details from Australian registered vessels. In theory, there are bilateral data interchange arrangements with other countries running their own LRIT systems. This is essentially a legacy system established after 911 and is now little used in practice.

9. But not including data from international flag state control systems or international port state control systems operated by AMSA, such as data from the Indian Ocean Computerised Information System (IOCIS) located in India, derived from safety inspections of vessels at ports of 22 Indian Ocean states that are parties to the Indian Ocean Port State Control MOU.
10. Following the disappearance of MH370, the Australian Department of Defence stated that the Jindalee radar network does not operate on a 24-hour basis except during military contingencies. In peacetime it is tasked to carry out specific jobs, but it does not continuously monitor the area to Australia's north and west (Bailey, 2016).
11. The AMIS was not without controversy when it was established. It was originally described as creating an obligatory 'Maritime Identification Zone', which led to fears that Australia may be claiming enforcement jurisdiction in international waters or within the claimed maritime zones of other states. This led to the reformulation of the system as a voluntary one (Klein, 2006).
12. The mission of ReCAAP is to 'analyse and provide accurate statistics of the piracy and armed robbery incidents to foster better understanding of the situation in Asia.' (ReCAAP ISC, u.d., p. 49)
13. The PRC's stated purpose is to 'raise awareness within the shipping industry of high risk areas with pirate attacks and specific ports/anchorages where armed robberies on board ships have occurred.' (ICC, u.d.)
14. The Singapore IFC's stated purpose is to achieve early warning of threats through collective awareness and threat assessment and provide actionable information for regional responses against maritime security threats.
15. Correspondence with author.
16. Renamed from the former 'Pacific Patrol Boat Program' as part of a greater emphasis on MDA.
17. This includes Australian-led intelligence, surveillance and reconnaissance (ISR) activities such as Operation Gateway, which has been in operation since 1981, focusing on the Malacca Strait, South China Sea and Bay of Bengal.
18. The Australian Maritime Safety Authority (AMSA) has recently engaged in a multi-year project to assist counterpart agencies in Mauritius, Maldives and Sri Lanka, involving training, staff exchange and the development of integrated national search and rescue centers. There is potential for a similar program focused on the development of integrated national MDA systems.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Dr David Brewster is a Senior Research Fellow with the National Security College. He is the author of numerous books and papers on Indian Ocean Security. His latest edited volume is *India and China at Sea: Competition for Naval Dominance in the Indian Ocean*. His latest report is Australia's Second Sea: Facing our Multipolar Future in the Indian Ocean.

References

Abbey, E. (2017). Australian defence signs $100 million deal for high-res satellite imagery. *Spatialsource.com*, 22 August 2014. Retrieved from https://www.spatialsource.com.au/remote-sensing/australian-defense-signs-100-million-deal-high-res-satellite-imagery

Asia Pacific Defence Reporter. (2011). Border security: Good operations and bad policy. *Asia Pacific Defence Reporter*, 14 March.

Australian Border Force. (2018). Border agencies working together to combat maritime security threats. 10 January. Retrieved from http://newsroom.border.gov.au/releases/border-agencies-working-together-to-combat-maritime-security-threats

Australian Customs and Border Protection Service. (2014). *Annual report 2013-14*. Australian Government, Canberra

Australian Government. (2013). Guide to Australian maritime security arrangements. Retrieved from https://www.homeaffairs.gov.au/AustralianBorderForce/Documents/GAMSA%202013.pdf

Australian Government. (2017). *2017 foreign policy white paper*. Canberra: Australian Government.

Bailey, B. (2016). MH370: search for missing Malaysian jet all but a farce. *The Australian*, 4 March.

Barnes, S. (2018). 'Air power and Australia's maritime domain awareness: In greek gods we trust. Canadian Forces College. Retrieved from https://www.cfc.forces.gc.ca/259/290/405/305/barnes.pdf

Baruah, D. (2018). India's evolving maritime domain awareness strategy in the Indian ocean. In D. Brewster (Ed.), *India and China at Sea: Competition for naval dominance in the Indian ocean* (pp. 162–174). Oxford: Oxford University Press.

Basu, N. (2017). India, Italy to form joint defence panel. *The Hindu Business Line*, 30 October. Retrieved from https://www.thehindubusinessline.com/economy/policy/india-italy-to-form-joint-defence-panel/article9932703.ece

Bateman, S. (2016). Maritime security governance in the Indian Ocean region. *Journal of the Indian Ocean Region*, *12*(1), 5–23.

Bateman, S., & Bergin, A. (2010). *Our Western Front: Australia and the Indian Ocean*. ASPI Strategy, March 2010.

Biddington, B. (2014). *Girt by Sea: Understanding Australia's maritime domains in a networked world*. Kokoda Paper No.10, November.

Boraz, S. C. (2009). Maritime domain awareness: Myths and realities. *Naval War College Review*, *62*(3), 137–146.

Brewster, D. (2018). New maritime governance and cooperation arrangements in the Eastern Indian Ocean: Challenges and prospects. In J. Schottli (Ed.), *Maritime governance in South Asia: Trade, security and sustainable development in the Indian Ocean* (pp. 117–130). Singapore: World Scientific.

Brewster, D., & Medcalf, R. (2017). Cocos and Christmas Islands: Building Australia's strategic role in the Indian Ocean. *Journal of the Indian Ocean Region*, 13(2), 155–173.

Bueger, C. (2015). From dusk to Dawn? Maritime domain awareness in Southeast Asia. *Contemporary Southeast Asia*, *37*(2), 157–182.

Bueger, C. (2017). *Policy brief: Effective maritime domain awareness in the Western Indian Ocean*. Institute for Security Studies Africa, Policy Brief, 4 July.

Bueger, C., & Bergin, A. (2018). Uniting nations: developing maritime domain awareness for the 'Blue Pacific'. *ASPI Strategist*, 8 May. Retrieved from https://www.aspistrategist.org.au/uniting-nations-developing-maritime-domain-awareness-for-the-blue-pacific/

Business Daily Africa. (2017). Kenya and India in deal to boost maritime security. *Business Daily Africa*, 17 January. Retrieved from https://www.trademarkea.com/news/kenya-and-india-in-deal-to-boost-maritime-security/

Daigle, L. (2018). Australia to upgrade long-range coastal radar network with BAE Systems, Defence Alert. 9 March. Retrieved from http://www.defencealert.com/defence-industry/64-bae-systems/23208-australia-to-upgrade-long-range-coastal-radar-network-with-bae-systems

Department of Defence. (2016). *2016 defence white paper*. Canberra: Australian Government.

Department of Defence. (u.d.). Operation solania. Retrieved from http://www.defence.gov.au/Operations/SouthWestPacific/

Equasis. (2016). The world merchant fleet in 2016 - Statistics from Equasis. Retrieved from http://www.emsa.europa.eu/equasis-statistics/download/5046/472/23.html

Government of India. (2016). Agreements for Exchange of White Shipping Information. 24 November. Retrieved from http://pib.nic.in/newsite/PrintRelease.aspx?relid=154221

ICC. (u.d.). IMB piracy reporting centre. Retrieved from https://www.icc-ccs.org/piracy-reporting-centre

Klein, N. (2006). Legal limitations on ensuring Australia's maritime security. *Melbourne University Law Journal*, *7*(2), 306–338.

Mugg, J., Hawkins, Z., & Coyne, J. (2016). *Australia's border security and unmanned maritime vehicles*. ASPI Special Report, July.

Munns, D. W. (2005). 121000 Tracks. *Sea Power*, 48(7) (July), 10.

Noonan, M., & Williams, E. (2016). Combating maritime transnational crime: An Australian perspective. *Journal of the Indian Ocean Region*, *12*(1), 46–51.

Phillips, J. (2017). Boat arrivals and boat 'turnbacks' in Australia since 1976. Parliament of Australia, 17 January.

Pomerleau, M. (2016). Info-sharing hurdles hinder alliance partnerships. *CS4ISRNet*, 7 August. Retrieved from https://www.c4isrnet.com/videos/2016/08/07/info-sharing-hurdles-hinder-alliance-partnerships/

Rahman, C. (2008). The global maritime partnership initiative: Implications for the Royal Australian Navy. Papers in Australian Maritime Affairs No. 24. Canberra: Sea Power Centre – Australia.

Rahman, C. (2010). Maritime domain awareness in Australia and New Zealand. In N. Klein, J. Mossop, & D. R. Rothwell (Eds.), *Maritime security: International Law and policy perspectives from Australia and New Zealand* (pp. 202–223). London: Routledge.

ReCAAP ISC. (u.d.). ReCAAP regional guide to counter piracy and armed robbery against ships in Asia (Singapore,undated), 49. Retrieved from http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Documents/ReCAAP%20Guide%20to%20Counter%20Piracy%20and%20Armed%20Robbery%20Against%20Ships.pdf

Royal Australian Navy. (2010). *Australian maritime doctrine: RAN doctrine 1 2010*. Canberra: Commonwealth of Australia.

Sputnick. (2017). India offers real-time intelligence data sharing with 10 countries. *Sputnick News*, 4 November. Retrieved from https://sputniknews.com/asia/201711041058816891-india-offers-itelligence-data-sharing/

Styles, B. (1998). JORN HF antenna arrays project completed. Retrieved from https://web.archive.org/web/20120206003705/http://www2.rfsworld.com/StayConnected/pdf/Stay2_98.pdf

Upadhyaya, S. (2017). A case for a pan-Indian Ocean information grid for improved maritime domain awareness. *Journal of the Indian Ocean Region*, *13*(3), 335–354.

US Government. (2004). National security presidential directive 41/homeland security presidential directive 13. *Maritime Security Policy*, 21 December.

US Government. (2005). *National maritime domain awareness plan*. Washington, DC: White House.