Contemporary Southeast Asia Vol. 37, No. 2 (2015), pp. 157–82 DOI: 10.1355/cs37-2a

ISSN 0129-797X print / ISSN 1793-284X electronic

From Dusk to Dawn? Maritime Domain Awareness in Southeast Asia

CHRISTIAN BUEGER

Information Sharing and Maritime Domain Awareness (MDA) are at the heart of the contemporary maritime security agenda. The goal of MDA is to develop shared understandings of developments and threats at sea. It is one of the preconditions for coordination and cooperation between diverse maritime security agencies and has often been understood as "key enabler". MDA is a major technical challenge in terms of collecting and fusing data and developing expert systems for the detection of anomalies. It is also a social, political and legal challenge. This study focuses on the latter. It asks how MDA can be organized and how the socio-political challenges can be addressed. The organization of MDA in Southeast Asia is discussed in-depth, with a focus on three major centres that are the backbone of the regional MDA structure. Although far from perfect, this regional system has become a role model for organizing MDA in other parts of the world. This article explores the functions that the three centres perform in the governance of maritime security in the region. I argue that each of the MDA centres has different strengths, and that their work should be seen as complimentary in an overarching system. The strength of the overall system is in enabling trust and being flexible and adaptable to the changing situation at sea. The conclusion outlines what lessons the system holds for the organization of MDA in other regions with a focus on the Western Indian Ocean.

CHRISTIAN BUEGER is Reader in International Relations at the School of Law and Politics, Cardiff University. Postal address: Cardiff University, School of Law and Politics, Law Building, Museums Avenue, Cardiff, CF103AX, Wales, United Kingdom; email: buegercm@cardiff.ac.uk; website: <http://bueger.info>.

Keywords: maritime security, information sharing, Maritime Domain Awareness, socio-technical systems, regional integration.

Maritime security is not only a contested concept, it also involves very different activities.[1] One of the major clusters of activities is that of information sharing. This domain has become central to coordinating national and international maritime security responses and to developing regional maritime security regimes. As America's National Research Council's Committee of the 1,000 Ship Navy phrased it, information sharing should be understood as a "key enabler".[2] It is a foundational practice, and has the potential to strengthen trust and confidence among maritime security actors. This in turn allows for joint law enforcement operations or even improved security relations between states in more general terms.

In the past decade various networks and centres for information sharing have become operational. Many of these are US-led efforts, such as the maritime security reports by the Office of Naval Intelligence, the Office of Global Maritime Situational Awareness or initiatives under the Maritime Partnership Concept.[3] Increasingly, however, regional initiatives have been developed, especially in the piracy prone areas of Southeast Asia, the Western Indian Ocean and West Africa. They have become important tools not only to tackle piracy, but to address maritime insecurity more broadly. Southeast Asia has spearheaded the development of regional MDA systems. The region has developed centres for information sharing which are both regional — in that they focus on Southeast Asian maritime zones — as well as global, since they work closely with non-littoral states and the global maritime players. The centres based in Singapore — the Information Sharing Centre (ISC) of the Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia (ReCAAP) and the Information Fusion Centre (IFC) operated by the Republic of Singapore Navy (RSN) —, and Malaysia — the Piracy Reporting Centre (PRC) of the International Maritime Bureau (IMB) — have become prototypes for how to organize regional information sharing. For the emerging architecture in other regions, such as the Western Indian Ocean as well as West Africa, these centres have become main reference points. Understanding how these centres work, and whether and how they can complement each other in a larger architecture, is hence a vital

task in order to improve a core dimension of maritime security provision. Scrutinizing these centres is also fruitful in academic terms, given that the centres represent a form of everyday practical international security cooperation which has hardly been studied. The centres imply that security actors engage in joint projects and interact on an everyday basis, which in turn might provide the preconditions of more sustained security interaction in the form of maritime security communities.[4]

This article presents a detailed analysis of the three regional Southeast Asian centres, and is divided into three parts. Following this introduction, part one discusses the challenges that information sharing networks and centres face. It foregrounds the importance of social and political aspects and suggests investigating information sharing by asking three questions: Among whom is information shared? What type of information and data is shared? And how is the information interpreted to gain shared understandings of the situation at sea? In the following section, each of the three Southeast Asian centres is discussed in the light of these questions. I argue that the centres should be understood as performing a range of different functions in a broader system. In the conclusion, I review the Southeast Asian system by addressing its efficacy and demonstrate how the overall system, rather than an individual centre, can serve as an international role model for organizing regional information sharing.

Understanding Information Sharing

"Information sharing" is a rather generic term. It refers to the transmission of data, information or knowledge across space and between individuals and organizations. The notion of "information" is often contrasted with the concepts of "intelligence" or "evidence", with the latter terms referring to information which is classified or not available in the public domain due to security concerns or ongoing criminal investigations and prosecutions. A further concept used in maritime security is that of "information fusion". This refers to attempts not only to distribute information, but to bring together and combine different sources in one stream. To organize information sharing for maritime security, two concepts have been developed: "Maritime Domain Awareness" (MDA) and "Maritime Situational Awareness" (MSA). Both refer to activities that lead to a shared picture and interpretation of what happens at sea. The US

government defines MDA as "the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States".[5] The maritime domain is defined 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".[6] Steven Boraz sketches out the width of tasks, when he argues that MDA

> means finding the ships and submarines of friends and foes, understanding the entire supply chain of cargoes, identifying people aboard vessels, understanding the infrastructures within or astride the maritime domain, and identifying anomalies and potential threats in all these areas.[7]

MDA and MSA grasp very similar activities. Yet, they have slightly different connotations and hence agencies differ over which term they use and how. MDA is the broader term, and, as given in the definition of the maritime domain above, goes beyond analysing what happens at sea, but rather focuses on everything connected to the maritime. In contrast, MSA emphasizes space and time (situations) and is hence more oriented towards operations, incidents, real-time analysis and rapid reactions. The focus of MSA is hence more directly related to understanding what is going on at sea. In consequence, MDA is often understood as the broader notion which subsumes MSA.[8] For the rest of this article I draw on this understanding and take MDA to be the broader, more encompassing concept interested in larger interpretations of developments at sea.[9]

The Challenges of Information Sharing

MDA is a major technological challenge. Big data from different sources and in different formats — satellites, radar, reconnaissance planes or humans — have to be stored and fused. Data need to be securely stored in central databases. User portals are required to make data accessible. Algorithms are needed for visualization, reporting, incident statistics or trend analysis. As Boraz phrases it, "massive amounts of data on all aspects of maritime activity must be collected, then cross-referenced, 'fused' (generally speaking, correlated across sources), and analyzed, in order to detect anomalies that may indicate threat-related behavior".[10] Developing this dimension will be an ongoing task for science and technology, and computer scientists specifically. MDA is, however, not a question of algorithms, software and technology alone. It also raises

questions about trust, identity, organizational cultures, interests and bureaucratic routines, as well as power constellations or political interests and how these shape MDA activities. MDA is hence a socio-political challenge, too. It concerns the willingness to share data, to engage in joint interpretation and to use these interpretations for action. To disentangle the socio-political dimension and the associated challenges, three questions need to be posed. First, among whom is information shared? Second, what information is shared? Third, by what mechanisms is a common interpretation or shared understanding of the information developed?

Which Actors are Involved in MDA?

MDA centres are confronted with the sheer number of agencies engaged in maritime security. Each of these maritime security agencies has a different organizational interest and culture, as well as different bureaucratic procedures. If this is already problematic on a national level, it is magnified on a regional or global level. The cross-sectorial nature of maritime security, moreover, implies a number of divides have to be bridged which have been identified as especially problematic. This concerns, firstly, the *civil-military divide*. Military actors are involved in maritime security and so are a broad range of civilian ones, ranging from police and border agencies to port authorities or environmental regulators. An impressive body of literature shows how difficult civil-military coordination is, given, for instance, misperceptions, or different cultures and routines.[11] Within a national as well as international context, e.g. in peacekeeping operations, it is often heavily contested whether civil or military agencies are in the lead. A second set of challenges relates to a *public-private divide*, that is, the coordination between state agencies and the shipping industry. Shipping is, by its very nature, a globalized industry. Because of the rise of open registries and the flag state principle of the United Nations Convention on the Law of the Sea (UNCLOS), shipping is a heavily self-regulated industry that often escapes state control[12] — although counter-terrorism provisions, such as the International Ship and Port Facility Security (ISPS) code have started to reverse this relationship.[13] In the volatile and highly competitive shipping markets, state regulations are largely seen as a cost factor. As a consequence, the industry often views state initiatives with suspicion. It is important to keep in mind that the state-industry relation varies over different maritime security issues. In the case

of piracy, the shipping industry is mainly a victim and hence more inclined to cooperate. With maritime security issues such as terrorism, illegal migration, the proliferation of weapons of mass destruction (WMD), or other questions of trafficking, the industry is to a lesser degree the core victim and is even a potential perpetrator. On these kinds of issues companies will be less likely to seek cooperation with states. These dimensions make the industry-state relation intricate. The problem is exacerbated by the rise of private security companies.[14] Many shipping companies prefer to pay for services such as maritime security reports or risk analysis, rather than relying on those provided by the state. Finally, if international information sharing is at stake, it is important also to be wary about *general political dynamics* between states, which is the third challenging divide. Maritime security information sharing does not operate in a vacuum. It is heavily influenced by the general relations between states and their national interests. Disagreements, tensions, historical friendships and animosities, alliances and cooperative agreements, or struggles over influence, all potentially shape the quality of information sharing in significant ways.

What Information is Actually Shared?

Information is a broad term that requires to be differentiated. The first basic type of information are reports of incidents at sea. Many incidents are in the public domain and reported by the media, so information sharing might only imply channelling such reports through a common network. Other reports might come from the maritime industry or law enforcement agencies. Reporting incidents will have certain regional geographical limits, might include territorial waters or only focus on the high seas. What type of incidents are included is the next question. Information sharing might be limited to one issue, for instance, to piracy, or include a broader range, such as fishery crimes, migration or smuggling incidents. Moreover, information might include only actual incidents, e.g. in the case of piracy, attempted and successful boarding, or also cover suspicious activities. How incidents are reported also differs in terms of the contextual information and the details provided. This includes also the question of whether post-incident data is provided, e.g. on the criminal investigations that follow, or whether prosecutions lead to sentences. The speed of sharing incident data has to be considered as well. If shared in real-time, incident data can be used for alerts as well as to coordinate responses. If

only shared as post-incident data, it is mainly useful for identifying trends and patterns.

A second layer of information concerns movements at sea in more general terms. Here the data provided by the international tracking systems is essential.[15] The Automatic Identification System (AIS) is a short range tracking system based on ship sensors, which have been compulsory since 2005 for any international voyaging ships with gross tonnage of 300 or more, according to the International Convention for the Safety of Life at Sea. The Long-Range Identification and Tracking (LRIT) system is a satellite-based ship tracking system compulsory since 2009 for passenger ships and cargo vessels above 300 gross tonnage engaged on international voyages. Both systems provide basic information on larger movements at sea. Other means of surveillance by satellites, air reconnaissance or radar are required to provide data sources for tracking smaller ships, such as fishing or leisure vessels, as well as the vessels not complying with international regulations. AIS and LRIT are internationally standardized and available data sources; beyond that data provision on movements at sea differs in terms of what kind of vessels (commercial, fishing, yachts, dhows, etc.) are included. It is also a question of more sensitive data such as on the employment of military assets and patrol vessels.

A third layer of information concerns more sensitive data, such as data from criminal investigations or intelligence operations, which can also potentially be shared in the frame of MDA. There are major hindrances in sharing this type of information. For the case of criminal investigations there might be legal concerns, and sharing information might hamper ongoing investigations. For intelligence data, one of the major problems is that countries often hesitate to share information since it might reveal information about their ability to collect intelligence.

By What Mechanisms is a Common Interpretation or Shared Understanding of the Information Developed?

As entailed in the US definition mentioned above, MDA is concerned about developing shared "understandings". Data and information does not speak for itself. A process of interpretation or "sense-making"[16] is required. A statement such as "12 piracy attacks have occurred in the Straits of Malacca in 2013" does not necessarily have meaning in itself. A problematization is required, that is, a claim about whether numbers are rising or in decline, whether more

needs to be done or a rapid response is needed. This also includes securitization processes, that is, to identify which events or actors are a threat to whom or what. The third analytical question is, hence, how do actors attempt to make sense of data and securitize? Various strategies are available to organize joint interpretation processes. Data can be interpreted through IT systems. Visualization techniques allow for the identification of geographical clusters, rule-based expert systems enable the identification of patterns and maritime anomaly detection, while databases for statistical analysis help identify historical trends. Interpretation can also be facilitated through dedicated research and analysis units, which interpret data on the basis of scientific methods, or via in-situ or Voice over Internet Protocol facilitated meetings in which data are jointly interpreted through the deliberation of participating actors.

In summary, the three questions — who, what, and how? — provide us with a productive framework for analysing MDA as a socio-technological challenge. The next section utilizes this framework to analyse the three main centres in Southeast Asia. The discussion draws on a reading of the documents of the centres, site visits and interviews with staff members as well as conversations with collaborators and users of the centres' information.

MDA in Southeast Asia: A Three-Centre System

Although drawing on US concepts and ideas, the development of *regional* MDA systems has been spearheaded by Southeast Asian actors. The region is an important case to understand how MDA can be organized, and what effects it has on maritime security provision and regional security cooperation. There are several reasons why Southeast Asia has assumed a leadership role in MDA. The first is that a significant proportion of global maritime trade is shipped through the region.[17] Secondly, along this critical maritime route, the South China Sea and the Straits of Malacca and Singapore saw a significant rise in piracy incidents from the 1980s onwards.[18] Piracy has remained a persistent problem in the region ever since.[19] Thirdly, the region is prone to considerable maritime interstate disputes due to the large numbers of contested geographical features (such as atolls, rocks and islands) and disputed maritime boundaries.[20] While one would expect that this is a hindrance for MDA cooperation, the opposite appears to be true. There is a high awareness for the importance of the maritime domain in general and the vulnerability of transport and economic growth.[21]

Three transnational centres for information sharing have been established in the region. The first was the IMB PRC founded in 1991. The ReCAAP ISC was opened in 2006, and the IFC inaugurated in 2009. All three centres engage in similar activities: they collect incident reports, compile incident data and disseminate them through IT networks, regular reports and events. Yet, they draw on very different structures, have a different approach, and as this article demonstrates, also perform very different functions (see Table 1). The difference in approach is already visible in the name of the respective centres: the PRC wants to "report", the ISC to "share", while the IFC intends to "fuse" information following ideas of contemporary MDA. The PRC and ISC are focused on piracy incident data, while the IFC takes a broader multi-issue maritime security approach.

Table 1
Basic Features of the Three Centres

	IMB PRC	*ReCAAP ISC*	*IFC*
Location	Kuala Lumpur	Singapore	Singapore
Legal Status	Non-governmental organization with observer status at IMO	Multilateral agreement and MoUs	Multi-bilateral agreements and MoUs
Funding	Voluntary contributions by insurance and shipping industry	Governments (core funding by Singapore)	Singapore Government (and other participating governments)
Coverage	Global piracy	Piracy in Southeast Asia	Maritime security incidents in Southeast Asia
Main Objective	Rapid operational response	Political consent	Operational coordination
Main Network	Shipping Industry & Law Enforcement Agencies	Nominated governmental focal points (civil focus)	Cooperating national maritime security agencies (military focus)

Source: Author.

IMB Piracy Reporting Centre (PRC)

The PRC is a body of the International Maritime Bureau (IMB) of the International Chamber of Commerce (ICC) and part of the ICC's broader work on countering organized crime and fraud. The IMB was founded in reaction to the first wave of contemporary piracy in the 1980s, notably around the South China Sea and the Straits of Malacca, as well as growing concerns over the impact of organized crime networks in shipping. Established in 1981, the IMB was tasked to "prevent fraud in international trade and maritime transport, reduce the risk of piracy, and assist law enforcement in protecting crews".[22] The International Maritime Organization (IMO) encouraged its members in a resolution to actively support the new organization. The IMB started to record piracy incidents in 1983 and has produced an annual report on piracy ever since. In 1991 the IMB extended its piracy work when it created the dedicated 24-hour PRC in Kuala Lumpur, Malaysia. The centre was intended to be the initial point of contact for shipmasters to report an incident of piracy. The main objective was to "raise awareness within the shipping industry, which includes the shipmaster, ship-owner, insurance companies, traders, etc., of the areas of high risk associated with piratical attacks or specific ports and anchorages associated with armed robberies on board ships",[23] but also to relay information immediately to local law enforcement agencies in order to ensure that shipmasters receive assistance.

The PRC "works and shares information with the IMO, various governmental, inter-governmental and law enforcement agencies including all industry bodies in an attempt to understand the nature of this crime and reduce its effects to crew, vessel and cargo".[24] The PRC is funded by voluntary contributions from shipping companies, insurance companies and industry-run Protection and Indemnity Insurance (P&I) Clubs, as well as grants from the governments of Taiwan and Cyprus.[25] As an industry-run organization, the PRC primarily works with and for the international transport industry. Indeed in many cases of piracy the PRC has been the first point of call for companies and incident data was distributed from the PRC to maritime security agencies and other information sharing centres. It distributes data on an ad-hoc, case by case, and needs basis if an incident is imminent in order to trigger a response. The PRC does not maintain a system of formal or official governmental contacts, such as a focal point system. As

already suggested by the task description, the PRC's work has also a considerable public dimension. It provides regular public available data and is one of the major public sources for piracy data and trend analysis. Since its inception the PRC has continuously advanced its reporting system. Starting out from the regular annual reports which were complimented by quarterly reports, in 2007 it launched a 24-hour maritime security hotline. Its dedicated public website not only provides the reports, but also current figures, as well as alerts and a "live map" of piracy incidents. The PRC is manned 24 hours by two staff and in addition twenty-five staff members run the day-to-day business. The PRC has an analyst in London who produces the reports, as well as a London-based director who conducts public advocacy work for the IMB. The backbone of the PRC is the so-called "IMB-PRC Worldwide Information System" through which data is stored, analysed and distributed. The PRC is linked to or has access to other information sharing networks, for instance the system provided by the IFC.

The PRC works without a geographical limit for its activities, and records and disseminates data on piracy across the globe. It reports all piracy incidents without a further categorization and does not differentiate between events occurring in territorial waters or on the high seas.[26] Hence it does not adopt the definition of piracy provided by paragraph 101 of UNCLOS, which sets strict geographical limits for piracy to occur in the high seas outside the 12 nm limit. The primary goal of the centre is to distribute piracy incident information in real-time to provide alerts for the shipping community as well as to organize operational responses to ongoing incidents. General MDA tasks are of secondary relevance for the PRC as its primary objective is to deal pragmatically with concrete events or regional patterns of incidents.

ReCAAP Information Sharing Centre (ISC)

The basis of the ReCAAP ISC is a formal multilateral (government-to-government) agreement finalized in November 2004 and which came into force in 2006. ReCAAP is a formalized and institutionalized form of cooperation and the ISC has the status of an international organization.[27] In addition to the ISC, ReCAAP is comprised of a Governing Council, which steers the work of the ISC, and a formal network of national focal points. ReCAAP has twenty "Contracting Parties" which includes the Southeast Asian littorals, but also

several European states (namely Denmark, the Netherlands, Norway and the United Kingdom) and Australia, Japan and the United States. It is funded by voluntary contributions. The main source of funding is provided by the Singapore government which pays for the office and key staff, while the other participating states mainly provide human resources.

The ISC's activities fall into three areas: a) collection, verification and dissemination of incident data; b) analysis and research of that data; and c) training, education and awareness raising. The cornerstones of the ReCAAP system are a national focal point system, an incident database, an Internet-based information sharing application, as well as sixteen staff based at the ISC's office in Singapore. ISC collects data on piracy incidents, mainly from the national focal points or from independent reports provided, for instance by the PRC, the IMO or the media. Data is then verified via the national focal points, shared throughout the network and later compiled into monthly and annual reports. In contrast to the PRC, the ISC distinguishes between piracy and armed robbery in accordance with the UNCLOS definition. It moreover classifies the significance of incidents into four categories, namely "very significant", "moderately significant", "less significant", and "minimum significant/petty theft".

The ISC operates a database and online information sharing portal. The portal has a mobile version that includes chat functionality, and also allows for the visualization of incidents on maps. The ISC also provides updates by participating in various events, including the quarterly Shared Awareness Meetings (SAM) of the IFC, the annual Nautical Forum based in Singapore, in which pre-versions of the annual reports are discussed, or in organizing events such as the scenario-focused annual piracy conference as part of the Singapore Maritime Week. ReCAAP has also provided substantial capacity building support, most notably by assisting with the establishment of the Eastern African Djibouti Code of Conduct Information Sharing Centers. The ISC connects different types of national focal points. Some countries have nominated security-oriented operational centres from navies or coast guards, others have nominated civilian maritime authorities, or search and rescue centres. The work of ReCAAP and its ISC is less operational in focus. As Ho notes, "this is because it receives information [...] from focal points, which necessarily means a delay in reporting".[28] Although the focal point system and information sharing portal allows

for the regional dissemination of reports, the ISC is not geared for maximizing speed or joint rapid responses to incidents. Its main function can be seen in raising awareness for piracy, and fostering a political consent on how the piracy situation in the region is developing. Arguably the level of trust that ReCAAP developed on a political level was an important pre-condition for developing the IFC three years later.

Information Fusion Centre (IFC)

The IFC was established by Singapore in 2009. It is an innovative centre that aims to develop a shared maritime security picture for Southeast Asia. This includes piracy hotspots such as the Straits of Malacca and Singapore, as well as the South China Sea. However, the IFC not only addresses piracy, but the broader spectrum of maritime security issues, including fishery crimes and maritime terrorism (but excluding interstate issues such as territorial and maritime boundary disputes). The IFC is located at Changi Naval Base. It consists of an operational room staffed 24/7 by the Singapore navy, a dozen offices for liaison officers and facilities for international exercises and simulations. The legal basis of the IFC are a series of Memoranda of Understanding (MoU) between Singapore and participating countries, as well as data sharing agreements with other MDA centres. Twenty-three countries participate in the IFC, of which fifteen presently have posted liaison officers. The IFC sense-making approach centres on two cornerstones: the liaison officer system and information technology. The liaison officer system, which is also used for coordination purposes in other multilateral naval headquarters (such as the European Union's EUNAVFOR), ensures that information can be passed on quickly and that shared evaluations of incidents can be developed in face-to-face interaction and daily meetings.

The IFC's information technology system is based on a kit of software titled the Open and Analysed Shipping Information System (OASIS). The system contains vessel information and tracks vessel movements on the basis of the AIS and LRIT. OASIS stores information on over a million vessels. It was developed by the Comprehensive Maritime Awareness Team from the Defence Science and Technology Agency (DSTA) of the Singapore government. OASIS draws on an open interface architecture that can be customized to different needs. In addition to the general MDA picture of the

IFC, OASIS also provides the basis for different customized portals. This includes portals for the Malacca Straits Patrols, the Regional Maritime Information Exchange of the Western Pacific Naval Symposium and the ASEAN Information-Sharing Portal. OASIS is web-based and a mobile version also exists. It also stores information on maritime security agencies and allows efficient communication through chat functionality. To further enhance communication the system also includes a live translation tool, by which chat messages are translated into other languages. OASIS also provides the data for an analytical tool called Sense-Making, Analysis and Research Tool (SMART). SMART allows the user to define rules and enables — as the developers describe it — to "piece together vague or partial information that spans organizational, national and time boundaries. SMART 'connects the dots' between real-time and archived data, thereby facilitating the investigation of vessels across time periods and identification of emerging trends."[29] Like other MDA software, OASIS/SMART is fully operational, but unfinished and requires continuous improvement. Its designers are working on integrating satellite and radar data, developing new predictive algorithms. These improvements will be required to address illegal fishing (given that vessels involved in illegal activities hardly have active AIS or LRIT), but also to ensure that in the process evidence is collected for prosecution and also the coordination between prosecutors is enhanced. The system does not have a mechanism to voluntarily report the location of naval and coast guard vessels which could be an important tactical tool to respond rapidly to incidents as well as to organize joint patrol and surveillance. OASIS successfully fuses information and SMART provides the analytical tools to map trends and identify potential issues. Combined with the face-to-face coordination of the Liaison Officers and the chat facility the IFC hence provides a sophisticated architecture for maritime security cooperation, rapid reaction as well as analysis. The IFC also organizes the quarterly Shared Awareness Meetings (SAM) which brings together the regional maritime security community to discuss current challenges (including partners such as ReCAAP, IMB and the shipping associations). In addition, the IFC is also engaged in education, training and exercises, for instance through organizing the ASEAN Maritime Security Information Sharing Exercise (inaugurated in July 2012), a week-long, bi-annual Maritime Security Practitioners course and regular workshops on maritime security.

Comparing the Centres' Functions

Contrasting the three centres — which are arguably very different in structure and approach — allows for understanding the advantages and disadvantages of each, but also how these add up to a larger functional MDA system for the region. Each of the centres has a different organizational form and handles information sharing differently. Table 2 summarizes the features of the centres.

As the brief introduction of each centre noted, officially the centres claim to do quite similar things. Yet, upon closer examination it is clear that the centres have different strengths. The PRC works in two different modes: in the crisis response mode it connects shipmasters with one (or several) law enforcement agencies; in the routine mode, it issues alerts, reports and statistics mainly for the shipping industry, but also the media. The PRC also frequently lobbies governments, especially if its analysis identifies emerging regional clusters of piracy incidents. By contrast, the ISC is less operative. Although it could develop this capacity, it does not primarily aim at organizing rapid responses to ongoing incidents. Instead, it ensures the everyday cooperation of the national focal points representing its members. Its primary function is hence in maintaining this network on an everyday basis. This has the effect of keeping attention for piracy high on government agendas and ensuring the political consensus that states act concertedly to address the problem. This consent is fragile, since national political priorities can change rapidly and piracy might not necessarily be a top political priority, or tensions between countries might arise that could challenge the willingness to cooperate. If the PRC is a private non-governmental organization, the ISC is a public international organization. The IFC in turn is equally a public, state-run organization, but does not have the formal status of an international organization. If the ISC is widely recognized to be a civilian organization, the IFC is much more military in character. It is run by the Singapore navy, and its liaison officers are defence officials, or officials who have a military background. The IFC mainly ensures communication between littoral and international navies and coastguards, and aims to enable shared operative responses by developing shared interpretations of the broader picture of maritime incidents. Like the PRC, the IFC is meant to provide rapid responses to incidents, yet in contrast to the PRC's ad hoc target approach of contacting law enforcement agencies directly, it works through official lines of command. Thus, all three centres are nodal points of different networks (see Table 3).

Table 2
A Comparison of the Three Centres

	Network/Audience	*Type of Information*	*Sense-Making Tools*
IMB **PRC**	▪ Private ▪ Ad hoc facilitation of connections between shipping companies and law enforcement agencies ▪ Broader public & media	▪ Piracy incidents	▪ Incident database ▪ Research & Analysis Team ▪ Statistics (Quarterly & Annual Reports) ▪ Real-time Visualization (live map) ▪ Events
Re **CAAP** **ISC**	▪ Multilateral (treaty) ▪ Focal points of national maritime security agencies (mainly civil) ▪ State representatives (Governing Council) ▪ Shipping Industry ▪ Broader public & media	▪ Piracy & maritime robbery incidents, classified into 4 categories	▪ Incident database ▪ Research & Analysis team ▪ Verification process ▪ Classification of incidents ▪ Statistics (Quarterly & Annual Reports) ▪ Consultation drafts ▪ Visualization ▪ Guidance documents ▪ Events (SAM, annual conference)
IFC	▪ Multi-bilateral (MoU based) ▪ Focal points of national maritime security agencies (multiple, mainly military) ▪ Shipping Industry	▪ 8 types of maritime security incidents (IUU fishing, piracy, irregular migration, arms trafficking, general maritime incidents, contraband trafficking, natural disasters, terrorism), ▪ Vessel Data (IMO, AIS, LRIT) ▪ Weather and Geographical Data	▪ Fused database of vessel information & incidents. ▪ Liaison Officers (in situ) ▪ Research & Analysis team ▪ Weekly reports ▪ Statistics (Quarterly & Annual Reports) ▪ Recommendations ▪ Real-time Visualization (live map) ▪ Rule-based expert system ▪ Events

Table 3
Main Networks of Centres

	Industry	*Media*	*Civil*	*Military*	*Governments*
PRC	+++	++	+	+	–
ISC	++	+++	++	+	+++
IFC	+	–	+	+++	+

Note: + indicates how heavily engaged the centre is with the respective actors.

The PRC and ISC are heavily engaged in the public domain, while the IFC has a much lower public profile. As a privately run organization, the PRC ensures that the industry, as one of the main victims of piracy, has a strong voice in the debate on piracy and maritime security. The ISC mainly works on a political level and guarantees the political will that government agencies shall work together. The IFC, firstly, embeds piracy in a larger maritime domain awareness context, and secondly, is much more operational in nature. Both the PRC and the IFC disseminate data in a very timely manner which allows for alerts and immediate incident responses. The ISC in turn ensures a political consent about incidents and trends in piracy through its verification process, but it also has a regulatory function in producing guidelines. Hence each of the centres performs a range of dedicated functions (see Table 4).

Table 4
Core Functions

	Incident responses	*Alerts & Early warning*	*Strategic Coordination*	*Best Practices*	*Symbolic*
PRC	+++	+++	+	–	++
ISC	–	+	++	+++	+++
IFC	+++	+++	+++	+++	+

Note: + indicates the capacities and involvement of a centre in a type of activity.

Another way to understand each centre's function is to ask how they have an effect on broader maritime security practice. This foregrounds the relative advantage of the state operated centres. The PRC can be seen primarily as having an effect on the quality of law enforcement operation, a function that the IFC also performs. Both the ISC and IFC contribute heavily to capacity building. They run

a range of capacity building activities such as training courses and workshops. The ISC, insofar that it is concerned about developing guidance documents, is also active in the domain of legal regulation, a role that is less clear in the case of the IFC. Both the ISC and IFC were created to positively impact on the quality of diplomatic relations between states. As one of the author's interlocutors phrased it, the goal is to make actors "comfortable" in working together. Both centres count states which understand each other as rivals or adversaries among its members, such as the United States and China. The collaborative experience of working through the centres has the potential for spillover effects on security relations in general. This may well alter the definition of national interests, and in the long run potentially influence the defence and national security dimension of maritime security.

Understanding the Southeast Asian MDA System

The three centres have different advantages and disadvantages. Yet, the point is not to argue about what one centre can do better (or worse) than the other. The question is how the three centres, if seen together, provide different functions in an overarching MDA system. Two characteristics of the system require further consideration: first the decentralization of the MDA across three rather than one centre; and second, the role of Singapore in the system.

One or Many Centres?

As Boraz argues,

> there is little doubt that no single entity or agency can be responsible for, or has the capacity to coordinate, all MDA-related activity. That fact, coupled with modern network-centric information capabilities, leads to a strong argument that 'nodes' generating maritime situational awareness must be linked.[30]

Having more than one centre is not only a technical necessity: it has various advantages. It ensures that awareness for piracy is high. Each centre reaches different audiences. The fact that several centres operate in the same "knowledge market" triggers competition. This, on the one hand, ensures that centres maximize their efforts. On the other hand, it also implies that there is a continuously significant public and professional presence of maritime security concerns, as the centres publish different alerts or reports. To maintain several

centres also allows for forum shopping: states or other actors who feel uncomfortable to engage in one centre can become active in another. For instance, the governments of Taiwan and Cyprus, both of which have an intricate legal status and their sovereignty is contested (by China and Turkey respectively), are core sponsors of the PRC. Malaysia and Indonesia do not formally participate in the ISC, but are contributors to the IFC. This ensures that all relevant stakeholders are actually engaged in the process, and legal hurdles or tensions given in one centre do not hinder the general participation in the system. The centres, as shown, also fulfil different functions, and it is doubtful that any single organization could perform all of them. A three-centre system is moreover flexible to make adjustments or adopt to the changing situation at sea. If new challenges arise, one of the centres will definitely be able to tackle the problem. The main weakness of a three-centre system — leaving aside the question of what would be the outcome of a cost-benefit calculation — is that there is a constant risk, that the centres, each operating under different definitions, classifications and reporting and verification standards, might come up with contradictory data or information.[31] What if the numbers differ or do not add up? The risk of what Sam Bateman describes as "monitoring wars"[32] can be mitigated, however, given that even in such a scenario, the outcome will be a public controversy which in turn implies further attention for maritime security and awareness that there is much at stake.

Network with a Dedicated Hub

For the overall system, it is noteworthy that it works with a dedicated hub. The fact that two of the centres are based in Singapore, and the other one is in the immediate vicinity, is instrumental for the system. The close proximity of the centres enables exchange between staff and joint events, such as the SAM meetings. Singapore is also a sense-making hub. The city-state hosts a significant academic community with strong expertise in maritime security based at institutions such as the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, the National University of Singapore (NUS) and the Institute for Southeast Asian Studies (ISEAS). Since MDA is above all concerned about shared interpretation and sense-making, independent experts can be vital in assisting in this process, in addition to the analysts working in the respective centres. Singapore, a wealthy island state, has not

only the funds to support MDA, but is also in the position to act as a governmental facilitator and honest broker easing interstate tensions. The role of Singapore in funding and hosting many of the activities, finally, also ensures that the system is de facto regionally owned. It is based on partnerships with international actors, such as China, Japan or the United States, but it is clearly run and steered by regional countries and not driven by external donor interests.

Lessons for Other Regions

What can we learn from the organization of the Southeast Asian MDA three-centre system? The lessons from the region are especially important for the Western Indian Ocean region, which in 2015 is at a critical juncture.

The Western Indian Ocean enters a time of transition with the international counter-piracy campaigns being fundamentally revised in the run up to 2016, when current military mandates expire. With the Djibouti Code of Conduct (DCoC) there is a mechanism in the region that has been designed to mirror ReCAAP in various ways. DCoC is not, however, fully functional. The majority of MDA functions, notably concerning piracy in the region, are currently organized by international actors and as such are not (yet) regionally owned. MDA is provided by the UK's Maritime Trade Organization based in Bahrain, which tracks ship movements and runs the central information sharing platform of the region, the so-called MERCURY system. The main naval missions in the region — NATO's Ocean Shield and EUNAVFOR's Operation Atalanta — provide alerts, incident data and reports. The Shared Awareness and Deconfliction (SHADE) Mechanism is a joint sense-making forum in which naval actors in the region together with the shipping industry meet on a quarterly basis. Whether and how these systems will be maintained in the event of a withdrawal of actors, once the current mandates come to an end, is the subject of much discussion.[33] Moreover, several other initiatives are underway which make the situation even more complex. A recent survey counts nineteen different institutions in the region, the majority of which carry an MDA component.[34] The two most important ones are the European Union's Programme to Promote Regional Maritime Security (MASE) and the UN Office of Drugs and Crime's (UNODC) regional maritime crime forum. The MASE project plans to build an MDA centre for the region as well

as an operational centre. Drawing on a software package developed by the EU, the intention is to install a system similar to that of the IFC. Given the EU's funding structure, MASE and its intended centre limits itself to work only with the African littorals, sidelining the Arabic and Asian littorals, notably Pakistan, India, Sri Lanka and Yemen. The other initiative, launched by the Maritime Crime Programme of the UNODC in 2014, plans to develop a network of regional law enforcement agencies to share best practices and information. Although the format is that of a forum, and the project does not envisage a centre, yet, it is designed to perform information sharing.

The system in the region will have to be organized in a more functional manner soon, and ensuring regional ownership will be important. The Southeast Asian experience can be an important guide, but one needs to acknowledge a range of substantial differences between the two regions. The first concerns capacities. The Western Indian Ocean littorals are in a much weaker economic situation and have less maritime capacities.[35] Only India, Pakistan and South Africa have significant blue water capabilities. While other countries are investing in naval and coast guard capabilities, this process will take time. Secondly, the Western Indian Ocean states have a weak regional identity. While there is a strong shared regional history dating back to ancient times, states do not have more recent experience in regional cooperation. The problem is accelerated by the multiplicity and overlap of regional integration mechanisms, none of which however stretches across the entire Western Indian Ocean.[36] There are however a number of core lessons that can be learned from the Southeast Asian system. These are obvious for the Western Indian Ocean, but prospectively also of relevance for the Gulf of Guinea, where a similar situation is developing. There are at least three major lessons.

Limit the number of centres: firstly, the number of centres that a regional MDA system requires is important. The region will require a network of (regional) centres, since no centre in its own right will be able to perform all functions required. As shown, the Southeast Asian system of three centres is functional, but constantly at risk of excessive competition. There is, however, an expected limit to the number of centres which are reasonable. With DCoC the Western Indian Ocean has already three ISCs and a training centre. UKMTO, NATO and EUNAVFOR also currently

conduct information sharing. If the planned MASE centre and the UNODC forum are added, this brings the total number to eight. This number appears unpromising and efforts are needed to limit the number of centres, focus their mandates and clarify their working relations.

A network requires a hub: secondly, even though a network of three to four dedicated centres for MDA in the region would be ideal, the Southeast Asian experience shows the importance of a "hub". Singapore is important in geographical terms for the system, since it allows for close working relations between centres, to organize meetings easily and cost-efficiently, but also to have a significant pool of independent (academic) experts present. The Singapore government also provides a solid funding basis for the centres and politically acts as an honest broker and facilitator between states. Which government and location could become such a hub for the Western Indian Ocean region requires consideration. Obvious candidates would be Bahrain (currently hosting SHADE), Madagascar (where the intended MASE centre will be built) or the Seychelles. Yet, these states lack capacities and do not have any significant academic expertise.

Balance international engagement and regional ownership: thirdly, the Southeast Asian example shows how MDA can be organized under regional leadership, while keeping international actors directly involved. With the Djibouti Code of Conduct (DCoC) the region has already a mechanism similar to ReCAAP; yet MDA is provided by international actors. In constructing a system for the Western Indian Ocean region it will be important to get the balance right. Some degree of overlap can be, as the Southeast Asian example shows, beneficial. However, there is an expected limit, and the region should not end up with five or more mechanisms. A crucial factor will be how the functions currently performed by SHADE will be embedded in regional organizations.

Conclusion: Organizing MDA

The question of how regional MDA systems can be organized, is vital for addressing maritime insecurity. MDA, as I have argued, is not primarily a technical challenge. If better technical solutions have to be developed the truly intricate questions are how

socio-political hurdles can be overcome, how the civil-military, the public-private, and interstate divides can be bridged, a culture of sharing developed and collective sense making be organized. The concept of MDA has often suffered from a bad image, and has been understood either as a hegemonic American project, or as an Aldous Huxley-style totalitarian technological project. It is neither. MDA has the potential to bring actors together. The Southeast Asian system documents the positive effects that a decentralized MDA system can have in ensuring collaboration across the civil-military, state-industry and interstate divides. It does not imply that the system can simply be replicated in other regions. Yet, it shows how a productive regionally owned system can be organized. Each region will have to draw its own lessons, but should pay close attention to the question of how far elements from Southeast Asia can be adopted. The cross-regional exchange of lessons and experiences is a promising route to take and academic analysis can play a vital role in this. The organization of MDA, as one of the core domains of maritime security practice, will require much further academic scrutiny. This will require cross-disciplinary conversations, notably between computer science and policy analysis. It will also imply to better understand how the everyday micro-interactions of MDA has meso or macro-level effects and alters the security relations between states.

NOTES

Acknowledgements: Research for this study has benefitted from a grant by the Economic and Social Research Council [ES/K008358/1]. I am grateful to the Centre for International Law (CIL) of the National University of Singapore for supporting my research and to my interlocutors in Singapore and Kuala Lumpur for taking the time to respond to my questions and facilitating visits. Previous versions of this paper were presented at the fourth Hudson Conference, Oxford University, March 2015 and at a CIL Seminar, May 2015. For comments and suggestions I would like to thank Ian Storey, Robert Beckman, Trine Villumsen Berling and the anonymous reviewers of *Contemporary Southeast Asia* as well as those asking critical questions at the two presentations of the paper.

1 Christian Bueger, "What is Maritime Security?", *Marine Policy* 53 (March 2015): 159–64.

2 National Research Council, Committee on the "1000-Ship Navy", *Maritime Security Partnerships* (Washington, D.C.: The National Academies Press, 2008).

3 See ibid.; Steven C. Boraz, "Maritime Domain Awareness: Myths and Realities", *Naval War College Review* 62, no. 3 (2009): 137–46; Chris Rahman, "Maritime

Domain Awareness in Australia and New Zealand", in *Maritime Security: International Law and Policy Perspectives from Australia and New Zealand*, edited by Natalie Klein, Joanna Mossop and Donald R. Rothwell (Abingdon, Oxon.: Routledge, 2010), pp. 202–23.

4 Christian Bueger, "Communities of Security Practice at Work? The Emerging African Maritime Security Regime", *African Security* 6, issues 3–4 (2013): 297–316.

5 *National Maritime Domain Awareness Plan* (Washington, D.C.: The White House, 2005).

6 Ibid.

7 Boraz, "Maritime Domain Awareness", op. cit., p. 141.

8 Ibid; Irvin Fang Jau Lim, *Comprehensive Maritime Domain Awareness: An Idea Whose Time Has Come?*, RSIS Working Paper No. 141 (Singapore: S. Rajaratnam School of International Studies, 16 October 2007), available at <http://www.rsis.edu.sg/rsis-publication/idss/141-wp141-comprehensive-maritime/#.VWk2z8scT5o>.

9 Although they are different concepts, it seems very difficult to provide clear definitions which would allow MDA and MSA to be clearly distinguished.

10 Boraz "Maritime Domain Awareness", op. cit., p. 139.

11 See the classical discussion in Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil–Military* Relations (Boston: Harvard University Press, 1981). An overview of the debate is provided in Peter D. Feaver, "Civil–Military Relations", *Annual Review of Political Science* 2 (1999): 211–41. Examples of civil-military challenges in contemporary operations are discussed in Lara Olson and Hrach Gregorian, "Interagency and Civil–Military Coordination: Lessons from a Survey of Afghanistan and Liberia", *Journal of Military and Strategic Studies* 10, no. 1 (Fall 2007): 1–48; and Iztok Prezelj, "Inter-Organizational Cooperation and Coordination in the Fight against Terrorism: From Undisputable Necessity to Paradoxical Challenges", *Comparative Strategy* 33, no. 4 (October 2013): 321–41.

12 See Susan M. Roberts, "Container", in *Globalization in Practice*, edited by Nigel Thrift, Adam Tickell, Steve Woolgar, and William H. Rupp (Oxford: Oxford University Press, 2014), pp. 85–87; and Helen Anne Sampson and Michael John Bloor, "When Jack Gets out of the Box: The Problems of Regulating a Global Industry", *Sociology* 41, no. 3 (June 2007): 551–69.

13 See Alexandros M. Goulielmos and Agisilaos A. Anastasakos, "Worldwide security measures for shipping, seafarers and ports: An impact assessment of ISPS code", *Disaster Prevention and Management: An International Journal* 14, issue 4 (October 2005): 462–78.

14 Carolin Liss, "The Privatisation of Maritime Security in Southeast Asia: The Impact on Regional Security Cooperation", *Australian Journal of International Affairs* 68, no. 2 (February 2014): 194–209.

15 For a discussion of these data sources and others that MDA wants to share and fuse, see Lim, *Comprehensive Maritime Domain Awareness*, op. cit.; Rahman, "Maritime Domain Awareness in Australia and New Zealand", op. cit.; Martin Murphy, "Lifeline or Pipedream? Origins, Purposes, and Benefits of Automatic Identification System, Long-Range Identification and Tracking, and Maritime

Domain Awareness", in *Lloyd's MIU Handbook of Maritime Security*, edited by Rupert Herbert-Bruns, Sam Bateman and Peter Lehr (London & New York: CRC Press, 2009), pp. 13–28; and Jan Georg Christophersen, "Satellite-based tracking of ships as global crime control: ISPS Code, AIS, SSAS and LRIT", in *Maritime Security in Southeast Asia*, edited by Kwa Chong Guan and John K. Skogan (London and New York: Routledge, 2009), pp. 146–61.

16 Lim, *Comprehensive Maritime Domain Awareness*, op. cit., p. 2.

17 Joshua Ho, "The importance and security of regional sea lanes", in *Maritime Security in Southeast Asia*, op. cit., pp. 21–33.

18 See Neil Renwick and Jason Abbott, "Piratical Violence and Maritime Security in Southeast Asia", *Security Dialogue* 30, no. 2 (June 1999): 183–96.

19 See Robert C. Beckman, "Combatting Piracy and Armed Robbery Against Ships in Southeast Asia: The Way Forward", *Ocean Development & International Law* 33, no. 3 (June 2002): 317–41.

20 See, for example, W. Lawrence S. Prabhakar, "The regional dimension of territorial and maritime disputes in Southeast Asia: Actors, disagreements and dynamics", in *Maritime Security in Southeast Asia*, op. cit., pp. 34–48.

21 Indicated not the least by attempts to develop regional maritime security regimes. See the evaluations in Sam Bateman, "Solving the 'Wicked Problems' of Maritime Security: Are Regional Forums Up to the Task?", *Contemporary Southeast Asia* 33, no. 1 (April 2011): 1–28; and John F. Bradford, "The Growing Prospects for Maritime Security Cooperation in Southeast Asia", *Naval War College Review* 58, no. 3 (Summer 2005): 63–86.

22 IMB Piracy Reporting Centre, available at <https://icc-ccs.org/piracy-reporting-centre>.

23 Ibid.

24 Ibid.

25 International Maritime Bureau (IMB), "Voluntary Sponsors", available at <https://icc-ccs.org/piracy-reporting-centre/voluntary-sponsors>.

26 Compare the critique of unclear legal classifications in Beckman, "Combatting Piracy and Armed Robbery Against Ships in Southeast Asia", op. cit., p. 332.

27 See Joshua Ho, "Combating Piracy and Armed Robbery in Asia: The ReCAAP Information Sharing Centre (ISC)", *Marine Policy* 33, no. 2 (March 2009): 432–34.

28 Ibid., p. 33

29 Defence Science and Technology Agency (DSTA), *The Comprehensive Maritime Domain Awareness Team*, 2010, available at <http://www.mindef.gov.sg/content/imindef/mindef_websites/topics/dtp/dtp2010/media/_jcr_content/imindefPars/download_3/file.res/6_dtp10_fs_tw_engg_cma.pdf>.

30 Boraz, "Maritime Domain Awareness", op. cit., p. 143.

31 See the discussion of Sam Bateman, *Piracy Monitoring Wars: Responsibilities for Countering Piracy*, RSIS Commentaries, no. 115 (13 May 2015).

32 Ibid.

33 "Oceans Beyond Piracy Facilitates Technical Sub Group on Maritime Situational Awareness", *Lessons from Piracy* website, 1 February 2015, available at <http://

www.lessonsfrompiracy.net/2015/02/01/oceans-beyond-piracy-facilitates-technical-sub-group-on-maritime-situational-awareness/>.

34 Christian Bueger and Jan Stockbruegger, "Maritime Security Governance in the Western Indian Ocean: A Survey", Corbett Paper, Corbett Centre for Maritime Policy Studies, Kings College London, forthcoming, 2015).

35 Ibid.

36 Ibid.