No. 141

Comprehensive Maritime Domain Awareness: An Idea Whose Time Has Come?

Irvin Lim Fang Jau

S. Rajaratnam School of International Studies

Singapore

16 October 2007

With Compliments

This Working Paper series presents papers in a preliminary form and serves to stimulate comment and discussion. The views expressed are entirely the author's own and not that of the S. Rajaratnam School of International Studies

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous School within the Nanyang Technological University. RSIS's mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education in international affairs with a strong practical and area emphasis

- Conduct policy-relevant research in national security, defence and strategic studies, diplomacy and international relations

- Collaborate with like-minded schools of international affairs to form a global network of excellence

Graduate Training in International Affairs

RSIS offers an exacting graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science (MSc) degree programmes in Strategic Studies, International Relations, and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Over 120 students, the majority from abroad, are enrolled in these programmes. A small, select Ph.D. programme caters to advanced students whose interests match those of specific faculty members.

Research

RSIS research is conducted by five constituent Institutes and Centres: the Institute of Defence and Strategic Studies (IDSS, founded 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2002), the Centre of Excellence for National Security (CENS, 2006), the Centre for the Advanced Study of Regionalism and Multilateralism (CASRM, 2007); and the Consortium of Non-Traditional Security Studies in ASIA (NTS-Asia, 2007). The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The S. Rajaratnam Professorship in Strategic Studies brings distinguished scholars and practitioners to participate in the work of the Institute. Previous holders of the Chair include Professors Stephen Walt, Jack Snyder, Wang Jisi, Alastair Iain Johnston, John Mearsheimer, Raja Mohan, and Rosemary Foot.

International Collaboration

Collaboration with other professional Schools of international affairs to form a global network of excellence is a RSIS priority. RSIS will initiate links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

ABSTRACT

The pelagic commons and littoral waterways that make up the global maritime domain are an over-exposed realm where international commerce remains vulnerable to threats to maritime safety and security. In an era where there is technological wherewithal and pressing security impetus to address the multifarious threats that emanate from the maritime domain, states can do more to work with international maritime organizations and captains of the maritime industry to develop and leverage upon the strategic locale of maritime hubs to develop regional maritime information sharing networks with potential global reach to safeguard the seas. The impetus for developing a comprehensive maritime domain awareness and information-sharing network is clear, and the tack to take would be to get buy-in on a building block regional approach.

Beyond the first important step of information sharing, the next bound that would be key to operationalizing such a maritime network would be that of information sense-making. In other words, comprehensiveness should lead to greater comprehension. This is an area of collaboration in sense-making that can help to develop a Community of Practice that aims to go beyond exclusive transactional notions of information exchange to that of a more inclusive open information-sharing praxis. If the challenges that remain can be overcome, 'need-to-know' maritime information sharing could well cross the Rubicon to one where 'responsibility-to-share' is manifested as an enduring public good.

****

Irvin Lim Fang Jau is an Alumni of IDSS-NTU. He graduated with an M.Sc. (Strategic Studies) – OUB Gold Medal 2000–2001. He has an MBA from Leicester University, U.K., 1999, and a B.A. (First Class Honours) in Communication Studies with University Medal in the Arts from Murdoch University, Western Australia, 1995. Irvin is also a top Distinguished Graduate of the U.S. Naval War College, Newport, Jan–Jun 2003. His research interests include foreign policy, critical security studies, the Revolution in Military Affairs, media studies and non-traditional security threats. He has published works covering geopolitics, military strategies and technology in the SAF Military journal *POINTER*, the U.S. ANSER *Journal of Homeland Security*. He has also written an article on communication theory and media praxis in an edited monograph on *Reading Culture: Textual Practices in Singapore* (1999) as well as one on water resource security in another edited monograph, *Beyond Vulnerability* (2002), with the Institute of Defence and Strategic Studies. He has previously published other Working Papers with IDSS on maritime security-related issues and military affairs.

Comprehensive Maritime Domain Awareness:
An Idea Whose Time Has Come?

> "There is *only* a perspective seeing, *only* a perspective 'knowing'; and the more affects we are allowed to speak about one thing, the *more* eyes, different eyes, we can use to observe one thing, the more complete will our 'concept' of this thing be."
>
> Nietzsche[1]

Introduction

In the Age of Exploration and Empires, where sailing into the unknown meant confronting certain peril, Henry the Navigator established a maritime centre in Lisbon to equip sailors with nautical knowledge, instruments and vessels to overcome the elements as they voyaged into new frontiers to discover new geographies of knowledge. Some 600 years later, with much of the seas well-charted and lands discovered, the idea of equipping sailors *and* maritime agencies with [fore]knowledge to overcome perils *at* and *from* the sea is no less germane. The perils confronting sailors, as well as nations of today and tomorrow, are trans-national in nature and multi-modal in trajectory. And they carry with them potentially grave [inter]national maritime safety and maritime security implications.

Such maritime threats include piracy, hijacking, the illicit trafficking of contraband and people, terrorism and the proliferation of weapons of mass destruction that find carriage and conveyance through the world's increasingly congested waterways. In particular, the terrorist threat in the maritime domain remains a clear and present danger. A successful terrorist strike on a major port or waterway would not only seriously disrupt global trade but also have a severe knock-on effect on many national economies dependent on the unimpeded flow of "right-on-time" maritime trade. Any deterioration in maritime security that results in the prolonged disruption or restriction of maritime trade along strategic waterways like the narrow and congested Malacca Strait—which accounts for a quarter of the world's maritime trade and 80% of the oil bound for China and Japan—can cause a hike in freight and insurance rates to exorbitant levels and severely disrupt the global supply chain. Dealing with

[1] See Friedrich Nietzsche, *On the Genealogy of Morals and Ecce Homo*, translated by Walter Kaufman & Reginald J. Hollingdale, New York: Random House, 1969 (p. 119).

such an expanded spectrum of maritime threats and scenarios, which are becoming increasingly trans-national and non-conventional in nature, demands greater international collaboration as well as domestic inter-agency coordination across the various informational, intelligence, operational and policy levels. To be sure, efforts to localize such maritime threats and their trajectories in the vast expanse of the world's waterways can be daunting, and may invariably end up like searching for the proverbial needle in a haystack. Nevertheless, there is operational utility for knowledge built around vessel-traffic tracking information that enhances the awareness in real time for priming responsive action against maritime threats. What is also equally clear is that no nation can go at it alone in such an expansive effort. There is therefore scope to build up relevant information-sharing expertise and capacity in order to facilitate more responsive collaboration between national agencies and the world's maritime centres to provide real-time visibility of the global flows of maritime traffic across the world's oceans.

The Need for Maritime Domain Awareness

Given the contiguous and porous nature of maritime boundaries, it is important to have effective surveillance of the world's waterways. Even if achieving "sea control" of the global commons in a Mahanian sense is but a will o' the wisp, the capability to "see and sense" what moves on water at any point in time is something that maritime nations can work together to achieve in order to improve marine safety as well as maritime security to safeguard their interests. It is now technologically possible to do so, even if technical hurdles remain. The key political challenge will be in securing the cooperation of countries to enmesh themselves in a web of maritime security information-sharing cooperation as a public good. Such information-centric cooperation will not merely be concerned with vessel traffic movement *per se* but will also need to drill down, with some measure of confidence, into important vessel-centric risk-profiling specifics like ownership, charterer, vessel cargo, crew manifests and even watercraft blueprints. Take the recent example of security concerns over almost 1,500 tonnes of explosives-grade ammonium nitrate used in mining operations that was shipped in and out of Botany Bay on five vessels that were registered in overseas ports such as Liberia, Antigua and Barbuda during the Sydney APEC summit in mid September 2007. The vessels had crews from Burma, the Philippines and Eastern Europe, and they had not undergone background security checks.[2] While ammonium nitrate usage on the mainland is heavily regulated, it is apparent that vessels carrying such cargo along coastal waterways are not. The shipments highlight the risks involved, calling into question potential blind spots and differing enforcement standards of regulatory regimes associated with foreign shipping entering a nation's waterways. Making shipping secure remains a big challenge for the international community, as much of the heavy-lifting of the globalized trading economy is performed by ships that fly under "flags of convenience", registered in tax havens with few minimum working conditions and differing standards of security clearance for crews. Achieving Maritime Domain Awareness (MDA) will require info-sharing, info-fusion and sense-making in order to cue responsive intelligence and operational coordination, as directed by decision-makers backed by relevant maritime legislation and shaped by strategy-driven policies.

The Quest Begins as an American Hot (Not Quite Trivia) Pursuit

The quest for the holy grail of *Domain Awareness* at sea is already well underway. In an ambitious attempt to better secure the over-exposed maritime domain, the United States has embarked upon a comprehensive national effort to enhance homeland security by preventing hostile or illegal acts within the maritime domain. The U.S. National Plan to achieve Maritime Domain Awareness was drawn up in October 2005 as one of eight supporting plans in operationalizing the National Strategy for Maritime Security (NSMS).[3] The central idea is to achieve an effective understanding of anything associated with the Maritime Domain that can impact the security, safety, economy or environment of the United States, and to provide warning or identification of threats as early and as distant from its shores as possible so that appropriate operational responses can be initiated in good time. Created as part of the December 2002 "Maritime Strategy for Homeland Security", the Maritime Domain Awareness (MDA) effort is to be driven by the United States Coast Guard (USCG) and Department of Homeland Security (DHS). The Department of Defense (DoD) also joined in

[2] The substance is well known as the terrorists' weapon of choice and was used in the bombings in Bali in 2002 and Oklahoma City in 1995. See Linton Besser, "Explosive Cargoes Steam by Airport", in *Sydney Morning Herald*, 5 September 2007.

[3] The NSMS is the pioneering comprehensive maritime strategy for maritime security, created in response to U.S. National Security Presidential Directive-41/Homeland Security Presidential Directive-13. See Wendy Kay, Stephanie McFadden & Matt Lincoln, "Global Maritime Integration: A Force Multiplier", *The ONI Quarterly*, January 2007, pp. 4–7.

the effort when it worked with the DHS to develop the complementary Global Maritime Intelligence Integration (GMII) plan as part of the NSMS.[4] Essentially, the MDA plan aims to construct a national Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR or C4ISTAR) capability for monitoring all ports, coasts and navigable waterways within the United States. The MDA initiative attempts to collect, analyse, assess and disseminate intelligence in support of defending the United States from maritime threats. Such an effort will entail persistent monitoring of the maritime domain, with information exchange via ready access to disparate databases for maritime knowledge sharing in order to build a Common Operating Picture for greater situational awareness. The U.S. Coast Guard has described it succinctly with the following heuristic as a shorthand: Global Maritime Intelligence (GMI) + Global Maritime Situational Awareness (GMSA) = MDA. As President Bush has well articulated for the American project: "The heart of the Maritime Domain Awareness program is accurate information, intelligence, surveillance, and reconnaissance of all vessels, cargo, and people extending well beyond our traditional maritime boundaries."[5] In many respects, the American MDA effort resonates with other mutually reinforcing global security initiatives that have been launched by the United States post-9/11, such as the Container Security Initiative, Customs Trade Partnership Against Terrorism (C-TPAT) and the Proliferation Security Initiative.

Connecting Virtual "Strategic Hubs": Vital Turnkey to CMDA Success

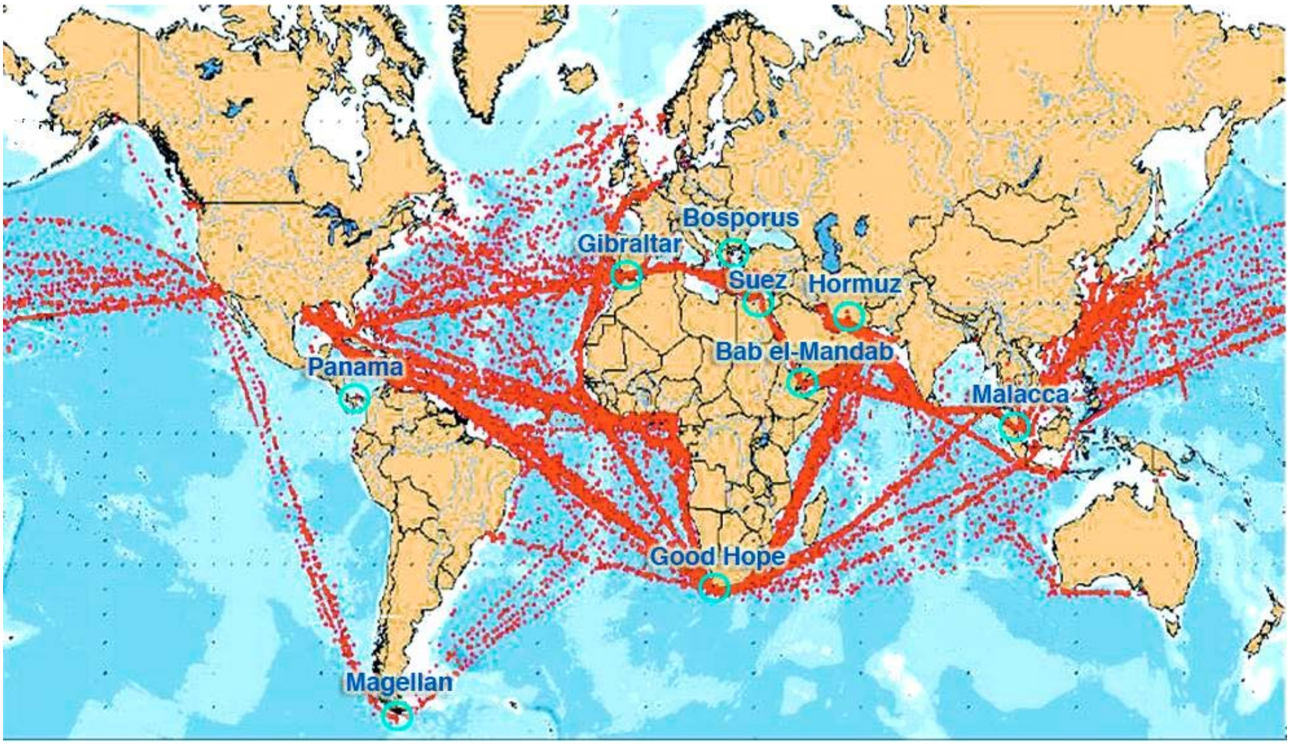
Beyond homeland security re-orientation and re-organization post-9/11, a key aspect of many of the above ground-breaking initiatives spearheaded by countries like the United States is the international dimension; the importance of recognizing and leveraging on multilateral cooperation that is inclusive remains the turnkey for success. Enhancing maritime security is not wholly a domestic concern of one state's national interest or responsibility, and states can ill afford to be provincial or parochial in tackling common maritime challenges that respect no borders. After all, many countries that depend on maritime trade for their survival also have active stakes in the safety and security of the seas and need to take *ownership in*

[4] The U.S. Office of Naval Intelligence (ONI) that has made an active pitch for its key role in GMII "considers the GMII to be a virtual global community of interest in which all U.S. intelligence agencies are stakeholders", ibid: 5.

[5] Speech (20 January 2002) cited in the "National Plan to Achieve Maritime Domain Awareness for the National Strategy for maritime Security", October 2005.

partnership. In other words, they can play a critical role in the overall effort to enhance maritime domain awareness by contributing their individual pieces of information within their respective maritime areas to complete the overall domain-awareness puzzle.

When one looks at the global maritime traffic patterns, it is clear that the key maritime centres located at strategic choke-points of maritime trade can serve as regional maritime information-sharing hubs for realizing MDA, or, in other words, introducing the ever-critical “C” for “Comprehensiveness” in the quest for a more watertight [inter]national MDA architecture.



Global Maritime Traffic Patterns and Strategic Choke-points

This can be done by adopting an incremental willing-partner “building-block” approach, with maritime hubs forging bilateral and multilateral intra-regional, information-sharing networks, even as they seek to link up with maritime regions beyond the region. All the while, the focus should be on making implementable steps that bridge targeted information gaps through information sharing rather than idealistic leaps that attempt to cover scattershot all information gaps and ultimately achieve little in addressing real maritime security threats.

Technology Watch

In recent years, quite a few watershed initiatives have been launched by maritime international regulatory bodies, like the International Maritime Organization (IMO), to promote marine safety by enhancing maritime awareness of seafarers around the world. These include some key developments that are reshaping the way vessel traffic information is being managed in the coming decade. These involve the proliferation of a shipborne Automatic Identification System (AIS), Long Range Identification and Tracking (LRIT) and Marine Electronic Highway (MEH) technologies worldwide as new international standards that enhance maritime domain awareness for seafarers and maritime agencies. Both the shipborne AIS and LRIT are IMO-mandated merchant shipping tracking instruments to enhance maritime domain awareness. These systems populate traffic data along waterways with the information collated and shared between merchant ships and shore-based maritime authorities. The systems are particularly useful in providing real-time traffic monitoring and tracking through busy and congested shipping lanes traversing through strategic maritime hubs around the world.

AIS: First developed in the late 1990's as a tool for navigation, the AIS, as specified by IMO, is a ship- and shore-based broadcast system, operating in the VHF maritime band. The AIS is designed to transmit a vessel's position and voyage data to other AIS-equipped vessels and shore-based authorities. In particular, information such as identity, position, course, speed, ship particulars and cargo information are exchanged between ships, as well as suitably equipped aircraft and shore stations. The system is designed to increase situational awareness and improve navigational safety through automatic reporting and short message exchanges in areas of mandatory and voluntary reporting schemes. It has been envisioned that the AIS facility could even enhance the safety of navigation by not only allowing vessels to quickly identify each other but also letting vessels de-conflict manoeuvring for collision avoidance as well by using the Digital Select Calling (DSC) facility. Further downstream, the AIS may be used to populate the Marine Electronic Highway (MEH)[6] project to be created along the world's strategic waterways, such as the Malacca Strait. The International Maritime Organization has mandated carriage requirements for VHF AIS on vessels that weigh more than 300 tons by 2007.[7]

Following heightened security concerns in the aftermath of the infamous September 11 terrorist attacks, Chapter V of the 1974 SOLAS Convention was amended to require mandatory carriage of AIS equipment on all vessels constructed on or after 1 July 2002 and mandatory operation at all times except where international agreements, rules or standards provide for the protection of navigational information. In view of the complexities involved in its implementation, a schedule was derived that provided for a phased-in implementation schedule for ships constructed before its expected entry-into-force date of 1 January 2008.[8]

[6] IMO has initiated a MEH project along the Malacca Strait.

[7] Reference: IMO SOLAS: 1974 and IMO Resolution MSC.99(73). As leisure crafts, fishing boats and other small boats of below 300 GWT are not required to be fitted with the AIS, there is a need to consider alternatives to track these vessels for a more comprehensive situational awareness, especially for smaller vessels operating within port limits and in the littoral waterways. For example, in what has been described as a world first, Singapore's Maritime Port Authority (MPA) has operationalized a Harbour Craft Reporting Transponder System (HARTS) for all MPA-licensed powered harbour and pleasure crafts of below 300 GWT, with effect from 1 January 2007, to facilitate the tracking of these crafts within Singapore port. The compulsory tracking device is designed to automatically track and monitor small vessels in Singapore's port waters and has been installed on board some 2,800 small crafts in Singapore to foil hijacking bids by terrorists or pirates. When the panic button is pressed, the authorities are immediately alerted to call for help. See "Maritime Security Exercise Highlights Anti-Piracy Device", *The Straits Times*, 24 August 2007.

[8] See "Types of AIS" by U.S. Coast Guard Navigation Center, available at www.navcen.uscg.gov/enav/ais/default.htm; and International Maritime Organization's AIS transponders information available at httred herringp://www.imo.org/Safety/mainframe.asp?topic_id=754.

Besides providing visibility on a range of different information types identified as “static”, “dynamic” or “voyage-related”. Static information is manually entered on installation and seldom changed, dynamic information is automatically entered from ship sensors. Voyage-related information is manually entered and updated as appropriate. Voyage-related information includes a ship’s draft, cargo type, destination and estimated time of arrival at the next port. A route plan, including way-points, can also be transmitted as well as short, safety-related messages.[9]

However, the range of access to AIS data is limited to between 20 to 30 nm, given the VHF maritime band on which it operates. Furthermore, access to AIS, being a broadcast system, is unrestricted. Therefore, there is the danger of manipulation such as false identification and false declaration of cargo that can go undetected, especially when they can be manually keyed into the AIS system of a ship.[10] The master of the ship is also empowered to turn off the AIS transmission due to security concerns.

LRIT: Concerns over limited range and security (information fidelity) are being addressed by implementation of LRIT, with IMO endorsing mandatory transmission of LRIT information through satellite in May 2006. For a start, LRIT data transmitted include positional, timing and merchant shipping identity details only.

The obligations of ships to transmit LRIT information and the rights and obligations of contracting governments and of search-and-rescue services to receive LRIT information have been established in regulation V/19-1 of the 1974 SOLAS Convention. The regulation dictates that there should be *no interface* between LRIT and AIS. Ships on international voyages that are required to transmit LRIT data include passenger ships, high-speed craft,

[9] See Australian Maritime Safety Authority (December 2003) Fact Sheet, available at www.armsa.gov.au/Publications/Shipping/AIS_fact.pdf; and MPA website at www.mpa.gov.sg/circulars_and_notices/pdfs/02-65.pdf.

[10] The pros and cons of the proposal by the U.S. Coast Guard (USCG) to use AIS as a means of surveillance for Maritime Domain Awareness is addressed by Captain (retired) Jay A. Creech and Captain Joseph F. Ryan in “AIS: The Cornerstone of National Security?”, *Journal of Navigation* Vol. 56, 2003, Cambridge University Press (pp. 31–44). See also “Letters to Editor: In the line of fire” in *Fairplay International Shipping Weekly*, 18 January 2007 and 4 January 2007, concerning controversial news uncovered by *Jane’s Navy International* that the Royal Navy is to purchase equipment that will allow them to transmit false AIS signals and possibly intercept, modify and resubmit calls from merchant ships.

cargo ships of 300 gross tonnage and upwards and mobile offshore drilling units. This regulation also establishes a multilateral agreement for sharing LRIT information for security and search-and-rescue purposes among SOLAS contracting governments in order to meet the maritime security needs and other concerns of such governments. For this purpose there are three categories of “states”. The “flag” state may track ships within its own fleet anywhere in the world. The “port” state may set its own requirements for ships that have indicated that they intend to call at its ports. “Coastal” states that belong to SOLAS contracting governments and have AIS shore-based installations are permitted to obtain tracking information for ships navigating within a distance up to 1,000 nm off their coast (applicable to ships not intending to call and not flying that state’s flag).

Although for now, by regulation, a merchant ship can only be tracked by a shore-based authority once it enters the 1,000-nm radius, the maritime situation picture can in fact be extended beyond 1,000 nm since it employs transmission via satellite. Even at an altitude of 800 km, it has been claimed that satellites should have little difficulty in picking up AIS transmissions. With global satellite coverage, it is not beyond the capability of some advanced nations to track all the movements of every one of the world’s fleet of AIS-equipped ships. Such extended coverage potentially expands the early warning bubble on suspicious Vessels-of-Interest (VOI) or Critical Contact of Interest (CCOI), while also extending merchant shipping information reach. What this translates to is greater policy sea-room and operational lead-time for states to capitalize upon the early warning time to plan and coordinate action in the event a VOI is identified, than previously possible.

As information transmitted through LRIT is limited to positional, timing and ship identity information, additional important layers of security information[11] that can be integrated into the system have yet to be adequately addressed. In addition, LRIT does not populate historical track data such as last ports of call. Most threat assessment matrices require such historical data to evaluate the threat level for a merchant ship.[12] While technology makes it possible for automatic tracking of ships calling at ports, this feature has yet to be utilized to populate security information in the LRIT system. Such information-sharing requirements are critical for more efficient target-profiling and effective risk

[11] Security information such as cargo and crew manifest and ISPS status declaration is not transmitted.

[12] The U.S. Coast Guard is reportedly working with satellite operator Orbcomm to develop its own LRIT system with the aim of obtaining historical data that the IMO-mandated LRIT system currently lacks.

management.

Despite such shortfalls and teething issues identified, the LRIT, when utilized in conjunction with the shorter range AIS feeding into the future MEH, would further accord greater transparency of the traffic, meteorological conditions and cargo passing through strategic waterways.

MEH: The Marine Electronic Highway (MEH) Project is an integrated system of innovative technological tools that also involves inter-governmental and inter-sectoral cooperative mechanisms for promoting maritime safety and protection of the marine environment.

In September 2005, Indonesia, Malaysia and Singapore signed a Memorandum of Understanding (MOU) with the International Hydrographic Organization (IHO) and the International Maritime Organization (IMO) to develop the MEH for the Straits of Malacca and Singapore. The MEH would utilize a network of official Electronic Navigation Chart (ENC) together with the Differential Global Positioning System (DGPS) and shipborne Automatic Identification System (AIS) to provide vital navigational information to ships, such as real-time tide and current readings.

An agreement to grant US$350,000 for the first phase of the development of a regional Marine Electronic Highway in the Straits of Malacca and Singapore was signed previously in March 2006 by the World Bank—acting as an implementing agency of the Global Environment Facility (GEF)—and the International Maritime Organization (IMO), the executing agency. The first phase is intended to lead to a multi-million dollar project to fully develop and implement the Marine Electronic Highway. The East Asia Regional MEH Project will have three phases, as follows[13]:

- Phase 1: A prototype system in the Straits of Malacca and Singapore
- Phase 2: Network construction in priority waters from the Straits to Japan
- Phase 3: Completion of the entire network with an emphasis on oil and gas transportation routes

A project office was established in Batam in July 2006 and resurveying work of the Malacca

[13] See Koji Sekimizu, Jean Claude Sainlos & James, N. Paw, *The MEH in the Straits of Malacca and Singapore: An Innovative Project for the Management of Highly Congested and Confined Waters*, London: IMO, July 2001; available at www.imo.org/includes/blastDataOnly.asp/data_id%3D3668/marineelectronichighwayarticle.pdf.

Straits will commence in 2007. Indonesia has also been granted funds to build shore-based AIS stations and acquire oceanographic buoys to facilitate their participation in the project.

From Share-Hubbing to Sense-Making

In the short intervening years post-9/11, shipborne AIS is already widely used at sea. Together with LRIT coming online, they form a simple yet powerful suite of ready-made maritime tools that can be used in conjunction with other maritime information systems and sensors (ashore and at sea) which are being developed to enhance maritime situation awareness and traffic management. More importantly, from the maritime security perspective, they can aid in the early identification and tracking of Critical Contacts-of-Interest (CCOIs) for possible maritime interdiction involving VBSS[14] operations.

Given that the technology to do such "virtual" borderless tracking via extra-terrestrial means (satellite) is already on the cards, potentially side-stepping sovereignty and territorial concerns, the next bound or growth area for international maritime security information-sharing collaboration may well be in the joint development and sharing of expertise in fusing all the information together in order to better sense-make the information deluge downloaded from the various systems. Comprehensiveness should lead to greater comprehension. For example, innovations in Risk Assessment Horizon Scanning (RAHS)[15] engines to pick up weak signals on mutating maritime threats at the macro scenario level can complement the development of advanced algorithms for delivering timely actionable threat evaluation at the operational contingency level.

Despite the profusion and possibly "confusion" over the many seemingly disparate MDA-enabling initiatives, the convergence of technological developments with heightened interest to operationalize global maritime information-sharing, coupled with investments in better sense-making capabilities, represents an opportunity to achieve Comprehensive

[14] Visit, Board, Search and Seizure (VBSS)

[15] Singapore has embarked on the development of RAHS that encompasses a unique combination of cutting-edge concepts, methodologies and technological solutions, and aims to provide policymakers with anticipatory knowledge of the nature of potential upcoming issues so that risks may be minimized and opportunities maximized. This whole-of-government enterprise is done by detecting "faint" signals, networking and linking the various governmental and private agencies, and fostering shared and informed analysis based on methodological diversity. The vision is that "RAHS will empower people with greater foresight to minimize the possibility of strategic surprises". See Barry Desker, cited in Barry Zellen, "Mitigating the Dangers of Strategic Surprise: Singapore Rises to the Occasion with RAHS", 2 April 2007, available at enterpriseinnovator.com/index.php?articleID=11114&sectionID=25.

Maritime Domain Awareness (CMDA). One signalling convergence effort is already being made in Southeast Asia by Singapore to be a proactive partner-of-choice in enhancing maritime security. Seating astride strategic cross-roads, with more than 50,000 vessels plying through the vital SLOCs of Southeast Asian waters annually and carrying about one-third of the world's trade and half of the world's energy supplies, Singapore is a "consequential place"[16] in the global maritime supply chain. The island state recently announced the building of its Changi C2 Centre[17] in late March 2007. This ambitious new facility, the first of its kind in the region, aims to serve as a regional maritime security hub when it is operational in 2009. It will provide a useful platform for nations to cooperate and respond more flexibly and effectively to a dynamic maritime security environment. Looking further ahead, it has the potential to develop into a strategic hub for a global CMDA network.

The Changi C2 Centre, a facility for multinational cooperation, built next to Changi Naval Base, is set to house three functional centres, namely, the Singapore Maritime Security Centre (SMSC), the Information Fusion Centre (IFC) and the Multinational Operations and Exercises Centre (MOEC). Envisioned to be the one-stop maritime information and response coordination centre to meet the maritime security needs of Singapore, this new centre will advance multi-agency cooperation and inter-operability among national maritime agencies and enhance Singapore's maritime security capabilities. The Changi C2 Centre will also enable international cooperation and inter-operability between countries to promote maritime security in the region.

The SMSC will bring elements of the Republic of Singapore Navy, the Maritime and Port Authority and the Police Coast Guard under one roof, to collate and maintain a comprehensive, 24/7 picture of the maritime situation surrounding the waters of the Singapore Straits. It will also serve as a command-and-control centre to coordinate and direct Singapore's responses to maritime security situations. The establishment of the SMSC is in line with Singapore's whole-of-government approach to dealing with maritime security challenges. Leveraging on the expertise and capabilities offered by these agencies, the SMSC will be able to maintain a round-the-clock comprehensive, real-time surveillance of the

[16] As described by Stephen Flynn in a discussion with him in Singapore (27 August 07). Stephen Flynn, an ex-USCG officer, is a Jeane F. Kirpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations. He is also author of *The Edge of Disaster: Rebuilding A Resilient Nation*, New York: Random House, 2007.

[17] See speech by Singapore Defence Minister Teo Chee Hean at the ground-breaking ceremony of Changi Command and Control Centre (27 March 1997), available at app.sprinter.gov.sg/data/pr/20070327984.pdf

maritime situation as well as coordinate and direct relevant operational responses to maritime security contingencies. The SMSC will plan its maritime security operations from a common room known as the Inter-Agency Coordination Centre in the event of maritime incidents or crises.

Beyond the home front, the Information Fusion Centre or IFC is envisioned to be a useful platform for fostering regional info-sharing cooperation among navies and other agencies. Intended to facilitate proactive sharing and fusion of information to enable analysis, planning and coordination of maritime responses in a more collaborative and networked manner, the IFC will be a centre where maritime information is collated and shared between international security partners to enhance awareness of the maritime security situation. To achieve this, it will house the necessary computer networks to fuse, analyse and disseminate information shared by participating civil-military agencies, heightening the maritime domain awareness of every participant plugged into the network. This will in turn help cue participating countries to take appropriate actions early to respond to potential threats.

While info-sharing enhances situation awareness, inter-operability among militaries and their civilian agencies is required to ensure that nations can work together effectively to respond to the dynamic security environment, a shared responsibility of common interest. To this end, the MOEC is being designed to be a conducive venue for militaries to interact in the planning as well as the command and control of forces and resources in various exercise settings. The MOEC will have a modern IT infrastructure with the necessary supporting command-and-control information systems to allow participating forces and agencies to operate together seamlessly. The MOEC will be able to support the planning and conduct of bilateral and multilateral exercises or operations. It could be used to enhance the conduct of large-scale multilateral exercises, such as the annual Five Power Defence Arrangements (FPDA) exercises and Exercise South East Asian Cooperation Against Terrorism (Ex SEACAT)[18], and function as a Maritime Security Centre for the conduct of regional maritime security operations, or as a regional Humanitarian Assistance and Disaster Relief Centre should the need arise. In anticipation of future contingencies, the MOEC has also catered additional space to provide additional capacity to meet any surge in future demands.

It is envisaged that Singapore’s Changi C2 Centre facilities will be extended to host

[18] Inaugurated in 2002, this is a U.S.-led annual multilateral anti-terrorism exercise that involves Brunei, Indonesia, Malaysia, Philippines, Singapore and Thailand.

foreign countries for multilateral or bilateral operations and exercises that serve to enhance regional inter-operability. In time, the Changi C2 Centre could become more than just a maritime security hub. It could even develop into a regional or global centre of excellence for maritime security.

A Domain Under Construction: Multiple Points for Multiple Fixes

The importance of networking coalition partners for any sustainable, credible and deterrent maritime security effort is also well-recognized in other maritime security cooperation related ventures. Take U.S. Chief of Naval Operations Admiral Mullen's eyebrow raising concept of the "1,000-Ship Navy" or what has now been termed the Global Maritime Partnership Initiative (GMPI) by the U.S. Navy (USN) as another telling example. The GMPI aims to make international maritime cooperation an important pillar of its new maritime strategy by building "a global maritime network to provide maritime security".[19] The call for a global network is an acknowledgment of the utility in better networking the community of navies around the world to enhance information sharing and promote inter-operability at sea. Implicit in the USN's "Thousand Ship Navy" (or GMPI) concept is the promising, if not polemical, metaphor of networking the power of a "Thousand Ships" from diverse partnering navies around the world—polling together of resources and expertise, sharing of information for collaborative sense-making and coordinating responses against common maritime threats.

Granted that GMPI is still at a conceptual stage, identifying funding, technologies, personnel, organization and modalities for ensuring better coalition inter-operability—at the sensitive but unclassified level—have yet to be ironed out. Nevertheless, the impetus for developing a C4ISR capability to realize comprehensive maritime domain awareness is clear.

To be sure, such networks already appear to be under construction—as U.S. Admiral Keating alluded to when he said that the USN is keen to exchange information and share databases with the Indian Navy to make international maritime security more robust.[20] Such fledgling bilateral proposals, should they translate into concrete initiatives over time by overcoming the various political and technical huddles, have the potential to kick-start and proliferate denser multilateral networks of maritime security information sharing further

[19] See George Galdorisi & Darren Sutton, "Achieving the Global Maritime Partnership: Operational Needs and Technical Realities", *RUSI Defence Systems*, June 2007, pp. 68–71.

[20] "Indo-US relation is Solid: US Admiral Keating", *ANI*, 23 August 2007.

downstream. In sum, multiple reference points provide for more accurate fixing, more reliable sense-making and more avenues for responsive action. For information sharing to take place, the U.S. military has developed its Combined Enterprise Regional Information Exchange (CENTRIX) system as one interoperable channel that can be used to promote its global maritime network—one that the USN has routinely used while operating with coalition forces at sea. It also has the more capable and secure Secret Internet Protocol Router Network (SIPRNet) for dedicated operational use when needed.[21] At the regional level, countries like Singapore have also developed their own unique ACCESS system for info-sharing to enhance inter-operability at sea, as well as the Internet-based Regional Maritime Information Exchange (ReMIX) portal under the *Western Pacific Naval Symposium* (WPNS) framework to promote wider information sharing among the navies of member countries.

Take the Malacca Straits as an example of how CMDA development can potentially take shape. In contrast to an earlier controversial U.S. proposal to enhance maritime security by deploying forces in the Malacca Straits via the "Regional Maritime Security Initiative",[22]—which subsequently turned out to be a catalyst of sorts in precipitating greater littoral state cooperation—the building up of a global maritime security network to achieve CMDA that includes the Malacca and Singapore Straits should be more politically acceptable and operationally realizable. Furthermore, with the anticipation that security along the Straits of Malacca would be strengthened when 10 new coastal surveillance radars, with sponsorship assistance by the United States, are installed along the eastern coast of Indonesia's Sumatra island in a couple of years[23], there may yet be new prospects for the sharing of situational picture in the Malacca Straits that can even be integrated into an expanded regional and global comprehensive maritime domain awareness network. Malaysia and Singapore have been running a comprehensive Vessel Traffic Information System (VTIS) for the Malacca

[21] See Christopher P. Cavas, "USS HMS Manchester, in Atlantic Exercise with USN, UK ships Take Unprecedented Role", *Defense News,* 6 August 2007, p. 4.

[22] The Straits of Malacca was the centre of a political storm in 2004 between the waterway's littoral states and U.S. Admiral Thomas Fargo, then Commander-in-Chief, U.S. Pacific Command, who had reportedly announced that under the Regional Maritime Security Initiative, the United States was planning to deploy marines and special forces in and around the strait to combat terrorism, proliferation, piracy, gun-running, narcotics-smuggling and human trafficking. See Vijay Sakhuja, "Malacca: Who's to Pay for Smooth sailing?", *Asia Times Online*, 16 May 2007. For more on the differing perspectives over this issue, see Ary Hermawan, "Malacca Coast Patrol to Stay Local", *Jakarta Post,* 26 August 2007, and "Who Owns the Malacca Straits", *Jakarta Post,* Editorial, 28 August 2007.

[23] See Eric Watkins, "Obstacles to Closer Counter-Terrorism Coordination in Malacca Straits", *Terrorism Monitor* Vol. 5 No. 13, 6 July 2007), The Jamestown Foundation, pp. 10–12; also available at www.jamestown.org/terrorism/news/article.php?articleid=2373531.

and Singapore Straits for more than a decade now, and any augmentation with Indonesia's entry into the extant arrangement from its side of the straits will no doubt further bolster maritime situation awareness, safety and security along the strategic waterways. Already, through their close cooperation in the Malacca Straits Coordinated Patrols and Eyes in the Sky at sea and from the air respectively, Indonesia, Malaysia and Singapore have shown that building a culture of maritime security cooperation between states can provide concrete operational results and political dividends in enhancing the maritime security along the Malacca and Singapore Straits.[24] Separately, Singapore and Indonesia have been successfully collaborating on Project SURPIC since 2005 to share the maritime situation picture to enhance surveillance and security of their common maritime borders along the Singapore Strait. Such multilateral and bilateral ventures demonstrate that, given sufficient political will, resource commitment and a balance of benefits for all involved, more can be done to shape and realize a more robust regional as well as global maritime security information sharing regime in the longer run. The new Singapore Changi C2 Centre that is being built is poised to be a key enabling node or hub in such a global CMDA network under construction.

Kick-start by Plugging into Extant Maritime Centres

There is scope for a comprehensively equipped maritime centre such as Singapore's Changi C2 Centre to link up and work with other [sub]regional maritime enforcement/information centres. For example, the U.S. National Maritime Intelligence Center (NMIC), headquartered in Maryland, is an operational outfit manned 24/7 by Office of Naval Intelligence (ONI) and U.S. Coast Guard personnel that enables the ONI to maintain a worldwide situational awareness on more than 18,000 ships on any given day.[25] Another facility is NATO's Allied Forces Maritime Component Command HQ Naples (CC-MAR Naples) that runs a Maritime Operations Centre. This Maritime Operations Centre, located close to the NATO Maritime Intelligence Coordination Centre, exchanges information with the national agencies of several NATO countries and works directly with NATO (Operation Active Endeavour) naval forces operating in the Mediterranean. It also exploits the synergies of sharing information

[24] Singapore, Indonesia and Malaysia have, in recent years, coordinated maritime and air patrols in the Malacca Strait. Pirate attacks in the Malacca Strait, which carries half the world's oil and more than a third of its commerce, have been on the decline since July 2005, with 11 cases reported in 2006. The improvement in maritime security has led to Loyld's JWC to rescind its declaration which resulted in the imposition of higher insurance premiums for ships transiting through the strait the year before.

[25] See "Q & A with RADM Richard Kelly", *ONI Quarterly*, January 2007, pp. 13–15.

with the experimental Joint Information and Analysis Centre (JIAC), which is structured as a fusion centre "to collect all available information and effectively collate, analyse and then disseminate data as actionable intelligence to the appropriate command".[26] In so doing, JIAC acts as an honest broker for fused information that protects the supply of nation's sources even as it passes, in a timely manner, its sense-made output to nations and agencies that are most likely to be able to exploit it.[27] Beyond establishing links with maritime security enforcement agencies, networking with other civil maritime safety and security set-ups should also be leveraged upon. One such other important centre that was launched (in late 2006), also based in Singapore, is the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia *(*ReCAAP) Information Sharing Centre (ISC).

ReCAAP was initiated by the Japanese Government in October 2001 as a multilateral cooperation and agreement initiative among the regional countries to combat piracy and enhance regional maritime security. The agreement was finalized in November 2004 in Tokyo and Singapore was proposed as the depository of the agreement and the host of the ISC. ReCAAP provides an important framework to enhance maritime security cooperation, information exchange and capacity building among the 16 member countries.[28]

As a key element of the ReCAAP agreement, the ISC is an international organization staffed by personnel from the members countries and managed by a Governing Council (GC).[29] The ISC facilitates communication and information exchanges between the member countries. It also collates and analyses information and intelligence from participating countries' Focal Points[30], affected vessels and companies, other organizations or

[26] See Vice Admiral Roberto Cesaretti, "Combating Terrorism in the Mediterranean", *NATO Review*, Autumn 2005; available at www.nato.int/docu/review/2005/issue3/english/art4.html

[27] See interview with Royal Navy's Chief of Naval Operations Admiral Sir Alan West, "Towards Maritime Domain Awareness", in *Asian Defence and Diplomacy*, Vol. 13 No. 2, February 2006, pp. 18–21.

[28] The 16 countries are the ASEAN States (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam), China, Japan, South Korea, India, Bangladesh and Sri Lanka. There are three categories of cooperative groups that ReCAAP will cooperate with, which the "member countries". Currently, 13 countries had signed and only 11 ratified the ReCAAP agreement, namely Cambodia, Japan, Laos, Singapore, Thailand, the Philippines, Myanmar, the Republic of Korea, Vietnam, India and Sri Lanka. Of significance, both Indonesia and Malaysia have yet to sign or ratified the ReCAAP agreement. However, both countries, being the member countries, will still be provided with the necessary information except that they will not be part of the Governing Council.

[29] The Governing Council is composed of representatives from each of member countries that have signed and ratified the agreements. It oversees the policies and guidance in the works of ReCAAP ISC and its members meet annually. The first meeting of the Governing Council of the ReCAAP Information Sharing Centre (ISC) was on 27–30 November 2006.

[30] The Focal Point is the point of contact for the contracting parties and can either be naval/coast guard personnel or port authority staff. They assist the ISC in the collection and management of information on

governmental agencies. The ISC also disseminates statistics, reports and information to the relevant member countries, parties and organizations, facilitating capacity building and offering of recommendations on follow-up actions and best practices. The ISC provides reports and assessment information on an ad hoc and periodic basis.

In order to facilitate information sharing to improve incident responses by member countries, analyse and produce reports on piracy and sea robbery incidents, and support capacity-building efforts among the ReCAAP member countries, the ReCAAP ISC has launched a web-based information sharing system, called Information Network (IFN) System, to operationalize the necessary exchanges and linkages with member countries. The web-based system has a public domain that provides general information on incidents and analyst reports for non-members and the general public, and a secured private domain that provides classified piracy information and analysis between member countries.

The ReCAAP IFN System is a 24-hour, secure, web-based information system that supports the ISC in the collection, organization, analysis and sharing of piracy and armed robbery information among member countries. It links up the ReCAAP ISC in Singapore with the designated Focal Points of ReCAAP member countries to enable the timely dissemination and exchange of maritime safety and security information. Besides Focal Points, ReCAAP ISC can also work in close partnership with other long-standing interested players like the International Maritime Bureau (IMB) Piracy Reporting Centre based in Kuala Lumpur, Malaysia, to achieve common objectives to improve marine safety and maritime security.

Although the ReCAAP ISC and Singapore's C2 Centre's IFC have different mandates and modalities of cooperation with their respective networks, their overarching mission to enhance maritime domain awareness through information sharing do not essentially differ. There is complementary scope for closer cooperation. The ReCAAP ISC facilitates communications, information exchange and operational cooperation between participating governments to improve incident response in order to combat piracy and armed robbery. The ReCAAP ISC also collates and prepares statistics and analyses of piracy and sea robbery

piracy and sea robbery incidents within their respective national territorial waters and jurisdiction, dissemination of information with the ISC, other Focal Points and their country's shipping community, facilitate investigation for their individual country law enforcement agencies and coordinate with neighbouring Focal Points for surveillance and enforcement actions on piracy and armed robbery against shipping incidents.

situation in the Asia region, and supports capacity-building efforts around the region. The ISC's IFN system's established links with the participating Focal Points represent a fledgling regional network that can be tapped upon and expanded further afield. This is an area where Singapore's C2 Centre's IFC can play a role, as it seeks to enhance maritime domain awareness of national maritime security agencies by fusing different sources of information (from its inter-agency network and partnerships in the region and beyond) and exploiting sense-making tools in order to derive a collated sea situation picture on piracy, terrorism and other risks and threats. Given the mutually reinforcing roles, there is scope for maritime security information-sharing agencies like the ReCAAP ISC to link up to share information with Singapore's future Changi C2 Centre's IFC, in an integrated CMDA architecture. Granted that it is still early days yet, and the fledgling ReCAAP ISC still has some way to go in building up research and real-time information-sharing capability via a distributed network of demonstrated operational utility. Nevertheless, should such promising developments live up to their potential, cooperative integration could kick-start the process for other maritime centres to be plugged into the information sharing network, and through its positive demonstration and exponential effect, cascade the growth of new offshoots linking up with other regional networks that contribute to the omnibus data-density of the envisaged CMDA project.

Grappling with Kinks in Information-Sharing

One paradoxical aspect of information sharing is dealing with the "tension" of information security at the other end. Information sharing may reveal sensitive sources and compromise surveillance capabilities that some partners or parties may need to safeguard or selectively make privy as a matter of organizational or national interest. Therefore, information sharing has to be secure, while partnerships are being secured, to allay any unease over the misuse and abuse of maritime security information. Related to these are governance and proprietary issues like whether there is a need for an "honest broker", or who gets to be the "system administrator" with "policing rights" for such a "detective" network, will need to be assuaged and addressed. What is clear is that the enabling technologies and evolving habits of cooperation need to be predicated on a relationship of trust with mutually binding agreements for partnerships in any shared venture to work. In the end, finding practical ways of enhancing bilateral and multilateral information-sharing cooperation could well mean defining mutually acceptable "rules of the game" for information sharing. These include data access-exchange policy, data integrity, source protection and collaborative tools that are capable of forming ad-hoc sharing through data links between shore-monitoring elements and surveillance assets at sea, as needed. In this regard, forging consensus over the governing parameters for the release of information with potential partners will be a vital first step before embarking upon any concerted effort at national and international levels to promote tangible maritime security info-exchange between willing and able partners from around the world.

Another hurdle relates to resistance against the introduction of additional layers of security information requirements with pervasive tracking facilities that are seen as little more than new-fangled security tools that could potentially complicate the lives of seafarers by adding transactional friction and cost to shipping operations. Such fears and perceptions, founded or unfounded, have real effects on the level of industry support. Given the slew of additional security measures that have been introduced in recent years,[31] a certain wariness by the world's commercial shipping community is to be expected and it will need to be assuaged. This is especially the case when significant commercial sensitivity *and* industry competition surrounds the availability of proprietary information regarding importers and exporters, the nature of cargo and the location of particular vessels. Over and above such market concerns, regulatory maritime regimes like UNCLOS and other related international conventions and customary international law also need to be appropriately reckoned with. This will be pivotal when framing the legal bases for securing buy-in on a viable CMDA project that critically needs to leverage upon industry participation and cross-boundary inter-agency collaboration.

In addition to managing such tensions, dealing with technical realities like connectivity issues between the various disparate systems, sense-making algorithms and system bugs will all require highly trained personnel with deeply-specialized knowledge to manage. In addition, how would the taxonomy of such a CMDA network look like and would it meet the needs of its users? The iterative adoption of an Engagement, Experimentation and Evolutionary Capability Development approach could be useful in preventing "white

[31] See Irvin Lim, "Not Yet All Aboard … But Already All at Sea over Container Security Initiative", *IDSS Working Paper* No. 35, October 2002, pp. 1–29; and "Fireball on the Water: Naval Force Projection-Protection, Coast Guarding, Customs Border Security and Multilateral Cooperation in Rolling Back the Global Waves of Terror … from the Sea", *IDSS Working Paper* No. 53, October 2003, pp. 1–30.

elephants" and avoiding the creation of a "museum of experiments", after all the collaborative effort and resource investments in realizing a common recognized sea situation picture. Nevertheless, in the emergent "competition" for the best practices and systems being developed to achieve a CMDA capability, some technical dead ends may well be necessary and only to be expected, with better innovative and cost-effective solutions overtaking and breaking new ground. Also, individual nodes in the CMDA network may well have specific requirements or limitations that lead to the incorporation of indigenous designs and processes that leverage on commercial off-the-shelf technologies *and* services as well. Already, commercially available options appear to have stolen the march on developing a rudimentary semblance of what an envisaged CMDA network could potentially look like. Vessel Monitoring Systems (VMS) established by regional fisheries management organizations, such as the South Pacific Forum Fisheries Agency (FFA) and the Commission for the Conservation and Management of Highly Migratory Fish Stocks in the Western and Central Pacific Ocean (WCPFC), are making use of satellite Global Position System (GPS) technology to automatically plot the movement of participating countries' fishing fleets.[32] In another more vivid global example, AISLive, which is available via subscription online, was established just barely a few years ago, in 2004, and now reportedly "covers over 1,200 places worldwide" with "more than 13,000 vessels under coverage at any one time". It does this by linking AIS information nodes around the world into a virtual maritime map. As an attractive commercial proposition, its "state-of-the-art viewing software" provides shipping companies with an easy means to track their fleets via what has been touted as "the most cost-effective method of tracking vessels in real time today".[33] This Internet-based facility represents an avenue for real-time tracking information on "white-shipping" that could be further harnessed. In terms of ready access to merchant shipping information, it should also be a path of least resistance insofar as CMDA is concerned.

In time, *network trust and technical-taxonomy challenges* associated with achieving CMDA should be surmountable. Whether a "standard fit" system-of-systems approach is

[32]. The 2005 Rome Declaration on Illegal, Unreported and Unregulated Fishing adopted by fisheries ministers calls for ensuring all large-scale fishing vessels operating on the high seas to be required by their Flag State to be fitted with VMS no later than December 2008. See Vessel Monitoring Systems, available at www.ffa.int/node/946; www.fao.org/fi/website/FIRetrieveAction.do?dom=topic&fid=13691; and www.wcpfc.int/pdf/Conservation%20and%20Management%20Measure-2006-06%20%5BCommission%20VMS%5D.pdf.

[33]. For access to the AISLive website, see www.aislive.com/

eventually adopted or not, for now at least, it appears that letting “a hundred flowers bloom” is the default and most practicable approach, with international organizations (governmental and non-governmental) in partnership with industry shaping system requirements and driving systems development. At some point downstream, when the various maritime information systems being developed around the world become online, the higher leverage *knowledge challenge* will be in aggregating and distilling the information deluge, by situating potential maritime threats “in context”. In other words, once the networks are in place, the real challenge or “delta” to be achieved after all the data gathering is sense-making. Sense-making is *the* value proposition of CMDA. Rather than “seeing threats everywhere” and sounding off with frequent false alarms that result in wasted effort, a CMDA sense-making system will need to be programmed with advanced and adaptive user-requirement algorithms that help to separate “the wheat from the chaff” in profiling, red-flagging and targeting CCOIs for timely alerts and appropriate action.[34] The development of threat evaluation matrices, anomaly detection and critical-path analysis capabilities will be critical to sense-making. Effective innovation in a collaborative sense-making enterprise to achieve CMDA will require close cooperation and fostering a culture of trust and habit of cooperation—not an easy feat, especially if it is to be done virtually, taking into account the differing perceptions of values, interests and sensitivity thresholds that can crop up to cloud the best of cooperative ventures, compounded by bureaucratic red tape across real-world national boundaries. Capacity-building and burden-sharing issues related to developing and maintaining a maritime information-sharing infrastructure can also pose additional political hurdles that should not be underestimated as they can potentially hamstring information-sharing and related sense-making efforts. In parallel with technical sense-making system development, training support and personnel development for the “sense-makers” will also need to be given due attention for analysts to develop deep subject-matter expertise in order to better customize requirements and exploit the range of tools provided by the various CMDA network systems to bridge information gaps and siphon out credible threats. Towards that end, the fostering of a Community of Practice (CoP) in a sense-making network built around maritime information-sharing hubs makes good sense. Such a maritime sense-making CoP will do well

[34] For example, the U.S. ONI has developed the Global TRADER cargo analysis tool kit. See Charles Dragonette, “Fitted for the Voyage: ONI Leads the Way in Global Maritime Intelligence Integration”, *The ONI Quarterly*, January 2007, pp. 8–12.

to “reify” a new knowledge ecology of open information-sharing that supplants knowledge economy notions of transactional information exchange, and in so doing, replace exclusionary notions of ‘need-to-know’ with an inclusive spirit of ‘responsibility-to-share’.

Going forward, even further downstream, assuming that some semblance of CMDA is eventually achieved, the CMDA project could well find new policy and operational-need to take on cross-domain and multi-modal challenges of tracking not just vessels at port or under way at sea. After all, the maritime domain is not just about what moves on the surface of the water, but also in the airspace above, and arguably what is about to be put to sea via land. In this regard, close interface or access to civil air domain awareness (air-space management) information may well be necessary. That said, taking on the next bound towards cross-domain awareness with the incorporation of additional domain awareness “overlays” will have to address capacity issues such as the infusion or broadening of personnel competency with cross-domain expertise, balanced against the risk of information overload vis-à-vis the dilution of focus. Until then, overcoming collaborative tensions associated with the collation and sharing of information, mutual sharing of insights into maritime security-related sense-making methodologies/logics, determining baseline information parameters to initiate action-able info-sharing cooperation, within and across national boundaries, to enhance maritime security should be challenge enough.

Conclusion

In a highly globalized world, where the political economy and strategic orientation of many nations are Merchantalist maritime, if not Mahanian maritime, achieving CMDA may well become a matter of “best national interest” for many trading nations who place a high premium on the unimpeded flow of global commerce and seek to safeguard the global commons for the international shipping community as a universal public good.

While the systems, schemes and modalities of cooperation have yet to be worked out, with many still at an early stage of development and “competition”, what has already been envisaged and rolling out in the pipeline should enable the many interested states, industry and other stakeholders around the world to better appreciate the benefits and opportunities that achieving CMDA represents, albeit balanced against resource commitment and costs involved. This should spur all parties to make the necessary investments and integration of best systems and practices in “a spirit of partnership”[35] to launch a new era—a maritime renaissance—of unprecedented marine safety and maritime security cooperation that is in the interests of the wider international maritime community as a whole, by actively contributing to the creation of a robust, reliable and resilient CMDA network—an idea whose time has *finally* come.

[35] For more on the need for navies to stay alongside the maritime industry in a spirit of partnership, see Geoffery Till, *Seapower: A Guide for The Twenty-First Century*, London: Frank Cass, 2004, p. 103.

IDSS Working Paper Series

1. Vietnam-China Relations Since The End of The Cold War (1998)
   Ang Cheng Guan

2. Multilateral Security Cooperation in the Asia-Pacific Region: Prospects and Possibilities (1999)
   Desmond Ball

3. Reordering Asia: “Cooperative Security” or Concert of Powers? (1999)
   Amitav Acharya

4. The South China Sea Dispute re-visited (1999)
   Ang Cheng Guan

5. Continuity and Change In Malaysian Politics: Assessing the Buildup to the 1999-2000 General Elections (1999)
   Joseph Liow Chin Yong

6. ‘Humanitarian Intervention in Kosovo’ as Justified, Executed and Mediated by NATO: Strategic Lessons for Singapore (2000)
   Kumar Ramakrishna

7. Taiwan’s Future: Mongolia or Tibet? (2001)
   Chien-peng (C.P.) Chung

8. Asia-Pacific Diplomac*ies:* Reading Discontinuity in Late-Modern Diplomatic Practice (2001)
   Tan See Seng

9. Framing “South Asia”: Whose Imagined Region? (2001)
   Sinderpal Singh

10. Explaining Indonesia's Relations with Singapore During the New Order Period: The Case of Regime Maintenance and Foreign Policy (2001)
    Terence Lee Chek Liang

11. Human Security: Discourse, Statecraft, Emancipation (2001)
    Tan See Seng

12. Globalization and its Implications for Southeast Asian Security: A Vietnamese Perspective (2001)
    Nguyen Phuong Binh

13. Framework for Autonomy in Southeast Asia’s Plural Societies (2001)
    Miriam Coronel Ferrer

14. Burma: Protracted Conflict, Governance and Non-Traditional Security Issues (2001)
    Ananda Rajah

15. Natural Resources Management and Environmental Security in Southeast Asia: Case Study of Clean Water Supplies in Singapore (2001)
    Kog Yue Choong

16. Crisis and Transformation: ASEAN in the New Era (2001)
    Etel Solingen

17. Human Security: East Versus West? (2001)
    Amitav Acharya

18. Asian Developing Countries and the Next Round of WTO Negotiations (2001)
Barry Desker

19. Multilateralism, Neo-liberalism and Security in Asia: The Role of the Asia Pacific Economic Co-operation Forum (2001)
Ian Taylor

20. Humanitarian Intervention and Peacekeeping as Issues for Asia-Pacific Security (2001)
Derek McDougall

21. Comprehensive Security: The South Asian Case (2002)
S.D. Muni

22. The Evolution of China’s Maritime Combat Doctrines and Models: 1949-2001 (2002)
You Ji

23. The Concept of Security Before and After September 11 (2002)
a. The Contested Concept of Security
Steve Smith
b. Security and Security Studies After September 11: Some Preliminary Reflections
Amitav Acharya

24. Democratisation In South Korea And Taiwan: The Effect Of Social Division On Inter-Korean and Cross-Strait Relations (2002)
Chien-peng (C.P.) Chung

25. Understanding Financial Globalisation (2002)
Andrew Walter

26. 911, American Praetorian Unilateralism and the Impact on State-Society Relations in Southeast Asia (2002)
Kumar Ramakrishna

27. Great Power Politics in Contemporary East Asia: Negotiating Multipolarity or Hegemony? (2002)
Tan See Seng

28. What Fear Hath Wrought: Missile Hysteria and The Writing of “America” (2002)
Tan See Seng

29. International Responses to Terrorism: The Limits and Possibilities of Legal Control of Terrorism by Regional Arrangement with Particular Reference to ASEAN (2002)
Ong Yen Nee

30. Reconceptualizing the PLA Navy in Post – Mao China: Functions, Warfare, Arms, and Organization (2002)
Nan Li

31. Attempting Developmental Regionalism Through AFTA: The Domestics Politics – Domestic Capital Nexus (2002)
Helen E S Nesadurai

32. 11 September and China: Opportunities, Challenges, and Warfighting (2002)
Nan Li

33. Islam and Society in Southeast Asia after September 11 (2002)
Barry Desker

34. Hegemonic Constraints: The Implications of September 11 For American Power (2002)
Evelyn Goh

35. Not Yet All Aboard…But Already All At Sea Over Container Security Initiative (2002)
Irvin Lim

36. Financial Liberalization and Prudential Regulation in East Asia: Still Perverse? (2002)
Andrew Walter

37. Indonesia and The Washington Consensus (2002)
Premjith Sadasivan

38. The Political Economy of FDI Location: Why Don't Political Checks and Balances and Treaty Constraints Matter? (2002)
Andrew Walter

39. The Securitization of Transnational Crime in ASEAN (2002)
Ralf Emmers

40. Liquidity Support and The Financial Crisis: The Indonesian Experience (2002)
J Soedradjad Djiwandono

41. A UK Perspective on Defence Equipment Acquisition (2003)
David Kirkpatrick

42. Regionalisation of Peace in Asia: Experiences and Prospects of ASEAN, ARF and UN Partnership (2003)
Mely C. Anthony

43. The WTO In 2003: Structural Shifts, State-Of-Play And Prospects For The Doha Round (2003)
Razeen Sally

44. Seeking Security In The Dragon's Shadow: China and Southeast Asia In The Emerging Asian Order (2003)
Amitav Acharya

45. Deconstructing Political Islam In Malaysia: UMNO'S Response To PAS' Religio-Political Dialectic (2003)
Joseph Liow

46. The War On Terror And The Future of Indonesian Democracy (2003)
Tatik S. Hafidz

47. Examining The Role of Foreign Assistance in Security Sector Reforms: The Indonesian Case (2003)
Eduardo Lachica

48. Sovereignty and The Politics of Identity in International Relations (2003)
Adrian Kuah

49. Deconstructing Jihad; Southeast Asia Contexts (2003)
Patricia Martinez

50. The Correlates of Nationalism in Beijing Public Opinion (2003)
Alastair Iain Johnston

51. In Search of Suitable Positions' in the Asia Pacific: Negotiating the US-China Relationship and Regional Security (2003)
Evelyn Goh

52. American Unilaterism, Foreign Economic Policy and the 'Securitisation' of Globalisation (2003)
Richard Higgott

53. Fireball on the Water: Naval Force Protection-Projection, Coast Guarding, Customs Border Security & Multilateral Cooperation in Rolling Back the Global Waves of Terror from the Sea (2003)
Irvin Lim

54. Revisiting Responses To Power Preponderance: Going Beyond The Balancing-Bandwagoning Dichotomy (2003)
Chong Ja Ian

55. Pre-emption and Prevention: An Ethical and Legal Critique of the Bush Doctrine and Anticipatory Use of Force In Defence of the State (2003)
Malcolm Brailey

56. The Indo-Chinese Enlargement of ASEAN: Implications for Regional Economic Integration (2003)
Helen E S Nesadurai

57. The Advent of a New Way of War: Theory and Practice of Effects Based Operation (2003)
Joshua Ho

58. Critical Mass: Weighing in on Force Transformation & Speed Kills Post-Operation Iraqi Freedom (2004)
Irvin Lim

59. Force Modernisation Trends in Southeast Asia (2004)
Andrew Tan

60. Testing Alternative Responses to Power Preponderance: Buffering, Binding, Bonding and Beleaguering in the Real World (2004)
Chong Ja Ian

61. Outlook on the Indonesian Parliamentary Election 2004 (2004)
Irman G. Lanti

62. Globalization and Non-Traditional Security Issues: A Study of Human and Drug Trafficking in East Asia (2004)
Ralf Emmers

63. Outlook for Malaysia's 11th General Election (2004)
Joseph Liow

64. Not *Many* Jobs Take a Whole Army: Special Operations Forces and The Revolution in Military Affairs. (2004)
Malcolm Brailey

65. Technological Globalisation and Regional Security in East Asia (2004)
J.D. Kenneth Boutin

66. UAVs/UCAVS – Missions, Challenges, and Strategic Implications for Small and Medium Powers (2004)
Manjeet Singh Pardesi

67. Singapore’s Reaction to Rising China: Deep Engagement and Strategic Adjustment (2004)
Evelyn Goh

68. The Shifting Of Maritime Power And The Implications For Maritime Security In East Asia (2004)
Joshua Ho

69. China In The Mekong River Basin: The Regional Security Implications of Resource Development On The Lancang Jiang (2004)
Evelyn Goh

70. Examining the Defence Industrialization-Economic Growth Relationship: The Case of Singapore (2004)
Adrian Kuah and Bernard Loo

71. “Constructing” The Jemaah Islamiyah Terrorist: A Preliminary Inquiry (2004)
Kumar Ramakrishna

72. Malaysia and The United States: Rejecting Dominance, Embracing Engagement (2004)
Helen E S Nesadurai

73. The Indonesian Military as a Professional Organization: Criteria and Ramifications for Reform (2005)
John Bradford

74. Martime Terrorism in Southeast Asia: A Risk Assessment (2005)
Catherine Zara Raymond

75. Southeast Asian Maritime Security In The Age Of Terror: Threats, Opportunity, And Charting The Course Forward (2005)
John Bradford

76. Deducing India’s Grand Strategy of Regional Hegemony from Historical and Conceptual Perspectives (2005)
Manjeet Singh Pardesi

77. Towards Better Peace Processes: A Comparative Study of Attempts to Broker Peace with MNLF and GAM (2005)
S P Harish

78. Multilateralism, Sovereignty and Normative Change in World Politics (2005)
Amitav Acharya

79. The State and Religious Institutions in Muslim Societies (2005)
Riaz Hassan

80. On Being Religious: Patterns of Religious Commitment in Muslim Societies (2005)
Riaz Hassan

81. The Security of Regional Sea Lanes (2005)
Joshua Ho

82. Civil-Military Relationship and Reform in the Defence Industry (2005)
Arthur S Ding

83. How Bargaining Alters Outcomes: Bilateral Trade Negotiations and Bargaining Strategies (2005)
Deborah Elms

84. Great Powers and Southeast Asian Regional Security Strategies: Omni-enmeshment, Balancing and Hierarchical Order (2005)
Evelyn Goh

85. Global Jihad, Sectarianism and The Madrassahs in Pakistan (2005)
Ali Riaz

86. Autobiography, Politics and Ideology in Sayyid Qutb’s Reading of the Qur’an (2005)
Umej Bhatia

87. Maritime Disputes in the South China Sea: Strategic and Diplomatic Status Quo (2005)
Ralf Emmers

88. China’s Political Commissars and Commanders: Trends & Dynamics (2005)
Srikanth Kondapalli

89. Piracy in Southeast Asia New Trends, Issues and Responses (2005)
Catherine Zara Raymond

90. Geopolitics, Grand Strategy and the Bush Doctrine (2005)
Simon Dalby

91. Local Elections and Democracy in Indonesia: The Case of the Riau Archipelago (2005)
Nankyung Choi

92. The Impact of RMA on Conventional Deterrence: A Theoretical Analysis (2005)
Manjeet Singh Pardesi

93 Africa and the Challenge of Globalisation (2005)
Jeffrey Herbst

94 The East Asian Experience: The Poverty of 'Picking Winners (2005)
Barry Desker and Deborah Elms

95 Bandung And The Political Economy Of North-South Relations: Sowing The Seeds For Revisioning International Society (2005)
Helen E S Nesadurai

96 Re-conceptualising the Military-Industrial Complex: A General Systems Theory Approach (2005)
Adrian Kuah

97 Food Security and the Threat From Within: Rice Policy Reforms in the Philippines (2006)
Bruce Tolentino

98 Non-Traditional Security Issues: Securitisation of Transnational Crime in Asia (2006)
James Laki

99 Securitizing/Desecuritizing the Filipinos’ ‘Outward Migration Issue’in the Philippines’ Relations with Other Asian Governments (2006)
José N. Franco, Jr.

100 Securitization Of Illegal Migration of Bangladeshis To India (2006)
Josy Joseph

101 Environmental Management and Conflict in Southeast Asia – Land Reclamation and its Political Impact (2006)
Kog Yue-Choong

102 Securitizing border-crossing: The case of marginalized stateless minorities in the Thai-Burma Borderlands (2006)
Mika Toyota

103 The Incidence of Corruption in India: Is the Neglect of Governance Endangering Human Security in South Asia? (2006)
Shabnam Mallick and Rajarshi Sen

104 The LTTE's Online Network and its Implications for Regional Security (2006)
Shyam Tekwani

105 The Korean War June-October 1950: Inchon and Stalin In The "Trigger Vs Justification" Debate (2006)
Tan Kwoh Jack

106 International Regime Building in Southeast Asia: ASEAN Cooperation against the Illicit Trafficking and Abuse of Drugs (2006)
Ralf Emmers

107 Changing Conflict Identities: The case of the Southern Thailand Discord (2006)
S P Harish

108 Myanmar and the Argument for Engagement: *A Clash of Contending Moralities?* (2006)
Christopher B Roberts

109 TEMPORAL DOMINANCE (2006)
Military Transformation and the Time Dimension of Strategy
Edwin Seah

110 Globalization and Military-Industrial Transformation in South Asia: An Historical Perspective (2006)
Emrys Chew

111 UNCLOS and its Limitations as the Foundation for a Regional Maritime Security Regime (2006)
Sam Bateman

112 Freedom and Control Networks in Military Environments (2006)
Paul T Mitchell

113 Rewriting Indonesian History The Future in Indonesia's Past (2006)
Kwa Chong Guan

114 Twelver Shi'ite Islam: Conceptual and Practical Aspects (2006)
Christoph Marcinkowski

115 Islam, State and Modernity : Muslim Political Discourse in Late 19th and Early 20th century India (2006)
Iqbal Singh Sevea

116 '*Voice of the Malayan Revolution*': The Communist Party of Malaya's Struggle for Hearts and Minds in the 'Second Malayan Emergency'
(1969-1975) (2006)
Ong Wei Chong

117 "From Counter-Society to Counter-State: Jemaah Islamiyah According to PUPJI" (2006)
Elena Pavlova

118 The Terrorist Threat to Singapore’s Land Transportation Infrastructure: A Preliminary Enquiry (2006)
Adam Dolnik

119 The Many Faces of Political Islam (2006)
Mohammed Ayoob

120 Facets of Shi’ite Islam in Contemporary Southeast Asia (I): Thailand and Indonesia (2006)
Christoph Marcinkowski

121 Facets of Shi’ite Islam in Contemporary Southeast Asia (II): Malaysia and Singapore (2006)
Christoph Marcinkowski

122 Towards a History of Malaysian Ulama (2007)
Mohamed Nawab

123 Islam and Violence in Malaysia (2007)
Ahmad Fauzi Abdul Hamid

124 Between Greater Iran and Shi’ite Crescent: Some Thoughts on the Nature of Iran’s Ambitions in the Middle East (2007)
Christoph Marcinkowski

125 Thinking Ahead: Shi’ite Islam in Iraq and its Seminaries (*hawzah ‘ilmiyyah)* (2007)
Christoph Marcinkowski

126 The China Syndrome: Chinese Military Modernization and the Rearming of Southeast Asia (2007)
Richard A. Bitzinger

127 Contested Capitalism: Financial Politics and Implications for China (2007)
Richard Carney

128 Sentinels of Afghan Democracy: The Afghan National Army (2007)
Samuel Chan

129 The De-escalation of the Spratly Dispute in Sino-Southeast Asian Relations (2007)
Ralf Emmers

130 War, Peace or Neutrality:An Overview of Islamic Polity’s Basis of Inter-State Relations (2007)
Muhammad Haniff Hassan

131 Mission Not So Impossible: The AMM and the Transition from Conflict to Peace in Aceh, 2005–2006 (2007)
Kirsten E. Schulze

132 Comprehensive Security and Resilience in Southeast Asia: ASEAN’s Approach to Terrorism and Sea Piracy (2007)
Ralf Emmers

133 The *Ulama* in Pakistani Politics (2007)
Mohamed Nawab

134 China’s Proactive Engagement in Asia: Economics, Politics and Interactions (2007)
Li Mingjiang

135 The PLA’s Role in China’s Regional Security Strategy (2007)
Qi Dapeng

136	War As They Knew It: Revolutionary War and Counterinsurgency in Southeast Asia *Ong Wei Chong*	(2007)
137	Indonesia’s Direct Local Elections: Background and Institutional Framework *Nankyung Choi*	(2007)
138	Contextualizing Political Islam for Minority Muslims *Muhammad Haniff bin Hassan*	(2007)
139	Ngruki Revisited: Modernity and Its Discontents at the Pondok Pesantren al-Mukmin of Ngruki, Surakarta *Farish A. Noor*	(2007)
140	Globalization: Implications of and for the Modern / Post-modern Navies of the Asia Pacific *Geoffrey Till*	(2007)
141	Comprehensive Maritime Domain Awareness: An Idea Whose Time Has Come? *Irvin Lim Fang Jau*	(2007)