MARITIME AFFAIRS Copyright © National Maritime Foundation
Vol. 5 No. 1 Summer 2009, pp. 39-56
Print ISSN: 0973-3159, Online ISSN: 1946-6609, DOI: 10.1080/09733150903121927

Routledge
Taylor & Francis Group
ANAMAYA
National Maritime Foundation

Long Range Identification and Tracking (LRIT) Apropos Global Maritime Security

Commander BK Verma IN*

Globalisation of the world economy and the interdependence of nations thereof, has ensured that the security of global maritime trade remains a priority security issue for the state administrations. Maritime terrorism, illegal arms and drug trafficking, piracy etc., continue to remain the scourge of trading nations. Visibility and identification through maritime domain awareness (MDA) has come to be universally recognised as the basic tenet of the process to ensure maritime security. In 2000, the International Maritime Organisation (IMO) decision for mandatory provision of automatic identification system (AIS) onboard merchant ships and International Ship and Port Facility Security (ISPS) compliance by ports served to significantly enhance maritime security. With increased perceptions of threat post 9/11, further measures were discussed to augment maritime security during the 2002 International Convention for the Security of Life at Sea (SOLAS) Conference organised by the IMO. The mandatory security measures, adopted in December 2002, included a number of amendments to the 1974 SOLAS. The Conference also adopted Resolution 3, for "further work by the IMO pertaining to enhancement of maritime security" and Resolution 10 for "early implementation of long range ship's identification and tracking (LRIT)." During the 81st session of the Maritime Safety

*Commander B.K. Verma IN is a Research Fellow with the National Maritime Foundation, New Delhi. He has been working specifically on ocean management issues for the last three years and, currently, is working on coastal security issues. The views expressed in this paper are those of the author and do not reflect the official policy or position of the National Maritime Foundation or the Indian Navy.

Committee, held at IMO Headquarters in London on May 10-19, 2006 regulations for LRIT were included in SOLAS Chapter V on Safety of Navigation. LRIT was made a mandatory requirement with effect from December 31, 2008 for merchant ships (over 300 gross registered tonnage – GRT) on international voyages and mobile offshore drilling units. LRIT entitles SOLAS Contracting Governments to receive information about ships navigating within a distance not exceeding 1,000 nautical miles (nm) off their coast. The regulation was scheduled to enter into force on January 01, 2009. Though the deadline of December 31, 2008 has elapsed, the implementation of LRIT could not be executed due to lack of conformity by all contracting nations. This paper deliberates on the concept of LRIT and traces its development while specifically exploring its relevance to India in terms of implementation and operation. At the threshold of entering LRIT enabled maritime awareness domain, it would be prudent for India to put in place procedures and infrastructure that will maximise the system output.

Over the last century, maritime activities have significantly contributed to the world economy. The same can be gauged by the fact that 90 per cent of world trade is carried by the international shipping industry.[1] Over time the total seaborne trade has quadrupled from just over 8,000 billion tonne-miles in 1968 to over 32,000 billion tonne-miles in 2007.[2] Figure 1 shows the trend of total seaborne trade. Constrictions along major ocean routes have given criticality to certain Straits and Channels that are commonly referred to as "choke points."[3] The implications for the United States (US) in terms of both trade and national security are so immense that these choke points, in certain quarters, have also been categorised as its natural resources.[4] In the post Cold War era, threats to maritime trade seem more likely to emerge from regional instability, piracy and non-state players than through conventional wars. Disruption in any of the critical routes due to these threats or any accident would directly impact the world economy and thereby the geo-strategic equations. The recent incidents of piracy in the Aden corridor are an apt indicator. Maritime terrorism, illegal arms and drug trafficking, piracy etc., continue to remain the scourge of many nations. Globalisation of the world economy and the interdependence of nations thereof has ensured that the security of global maritime trade remains of critical importance to governments.

Initiatives for Enhancing Global Maritime Security

In order to enhance maritime safety, in 2000 the IMO adopted a new requirement to provide identification at sea. The requirement was to carry onboard ships an automatic

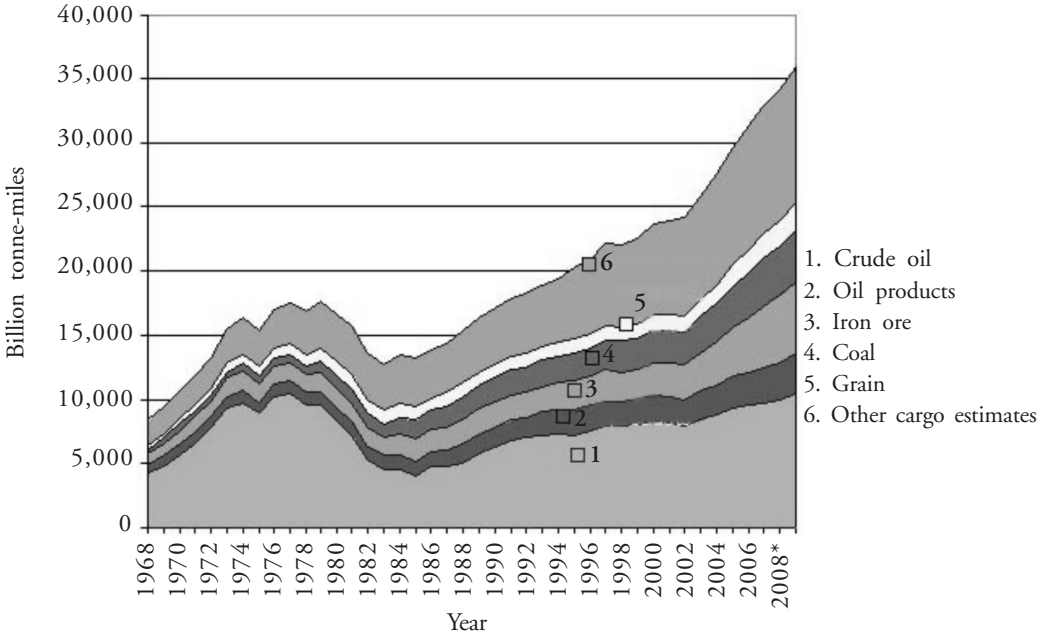

Fig. 1. Total seaborne trade;[1] *estimated.

identification system (AIS), capable of providing its positional and identification information to other ships and to coastal authorities automatically.[5] This requirement was made compulsory through a revised new Chapter V of SOLAS. The AIS is mandatory for all ships above 300 GRT engaged on international voyages as also cargo ships above 500 GRT not engaged on international voyages. It is applicable to all passenger ships, irrespective of size. The requirement became effective on December 31, 2004 and mandated ships to maintain AIS in operation at all times except where international agreements, rules or standards provided for the protection of navigational information. The enabling of AIS, a very/ultra high frequency (V/UHF) range system (approximately, 30-50 nm), immensely improved the visibility and identification of ships at sea. Primarily meant to address maritime safety, AIS has been increasingly utilised in the last few years to enhance vessel traffic management services (VTMS) and also maritime domain awareness (MDA) in coastal areas. Several nations such as Norway,[6] Turkey, Australia and several others have set up coastal AIS stations to monitor the traffic transiting within 40-50 nm off their coast. In India, too, there is a proposal for establishment of a National Automatic Identification System Network with 85 base stations.[7] The Directorate General of Lighthouses and Lightships (DGLL),

Government of India, which is steering the project, put forth the proposal in 2006. However, the same is still on the drawing board and a detailed report has been submitted only towards the end of 2008.

Advance Notice of Arrival (ANOA)

Following the attacks of September 11, 2001 (9/11) on the US, three forms of maritime terrorism have been identified as causes of concern – direct attack on a ship, hijacking of a ship carrying dangerous cargo, and the use of a ship as a 'weapon' to attack port or land facilities.[8] Shortly after 9/11, the US enforced a conditionality of prior intimation for any merchant ship intending to enter US waters through Advance Notice of Arrival (ANOA) requirements. The US Coast Guard (USCG), under the National Vessel Monitoring Centre, requires a 96 hour ANOA for any vessel intending to enter a US port or place of destination.[9] Failure to submit an ANOA results in the vessel being delayed and/or subjected to civil penalty proceedings. The success of this programme has been ensured through strict enforcement measures, which required surveillance and coordination. Thus, it is absolutely essential that any measure to regulate maritime activity requires adequate and capable enforcement infrastructure.

Container Security Initiative (CSI)

The rise in the world container shipment traffic along with susceptibility of the port infrastructure only "enlarged the gap" in the security setup. The fact that ships operating under flags of convenience (FoCs), whose norms are liberal, hold a significant percentage of the world shipping tonnage only makes the threat significant. With its large dependence on containerised trade, the US sought to address the issue through the Container Security Initiative (CSI).[10] The CSI was developed by US Customs, now the US Bureau of Customs and Border Protection (CBP), in the wake of 9/11.[11] The CSI addresses the threat to border security and global trade posed by the potential for use of a maritime container to deliver a weapon.[12] The initiative aims to identify and check more than 230 million cargo containers (shipped annually to the US) before they reach the US shores,[13] for possible threats – weapons of mass destruction (WMDs) or dangerous radioactive substances – that could be transported through these containers. In 2007, the US Congress adopted a radical unilateral requirement for 100 per cent security scanning by 2012 of each and every in-bound maritime container, to be conducted at the port of loading overseas.[14] The CSI is now operational at ports in

North America, Europe, Asia, Africa, the Middle East, Latin America and Central America. Over 58 operational CSI ports now handle approximately 86 per cent of all maritime containerised cargo imported into the US subject to pre-screening prior to importation. The World Customs Organisation and the G8 countries have supported CSI's expansion through their adoption of resolutions that support the implementation of the security measures introduced by CSI at ports throughout the world. One such conditionality of the CSI requires officials of the US CBP to be posted at the ports in other countries. Till date, Canada and Japan are the only two countries to have exercised this option. The Jawaharlal Nehru Port Trust (JNPT), India's largest container terminal, became the first port in the country to sign this global security initiative.[15]

Proliferation Security Initiative (PSI)

The Proliferation Security Initiative (PSI) is another element of the 2002 US national strategy to combat WMD proliferation, which calls for a comprehensive approach to counter the threat of WMD reaching the hands of terrorists.[16] Frustrated efforts to prevent the delivery of a shipment of North Korean SCUD missiles to Yemen in December 2002, added further impetus to PSI's launch. President George W. Bush formally announced the initiative on May 31, 2003 in Krakow, Poland. The PSI is an activity, not an organisation. Its objective is to interdict WMD, or WMD related shipments, between source countries, terrorist organisations and state recipients on land, in the air and on the high seas. Starting with 11 participants, the initiative now also includes Canada, Denmark, Norway, Singapore and Turkey, which joined in January 2004. The entry of the Russian Federation in June 2004 brought 'membership' to its current figure of 17 nations. However, the US claims that more than 70 states have expressed support for the PSI, with Argentina, Iraq and Georgia the latest to do so. A number of non-participant countries like Pakistan, too, have joined PSI exercises as observers. However, many countries, including India, have remained aloof from embarking on this initiative.

International Ship and Port Facility Security (ISPS)

With the intent of gathering larger participation from the world community, the US and other nations deliberated on means to enhance maritime security at the IMO. The same was discussed during the development of special measures to enhance maritime security during the 2002 SOLAS Conference. The mandatory security measures, adopted in December 2002, included many amendments to the 1974 SOLAS.[17] One such

amendment pertains to the International Ship and Port Facility Security (ISPS) Code.[18] Ship and port facility security is a risk management activity wherein action could be taken to eliminate the source of the threat, or an alternate risk reduction approach could be adopted to lessen possibilities to the lowest practicable. The ISPS Code provides a standardised, consistent framework for managing risk and permitting the meaningful exchange and evaluation of information between contracting governments, companies, port facilities, and ships. The comprehensive security regime for international shipping entered into force on July 1, 2004. The Conference also adopted Resolution 3, for "further work by the IMO pertaining to enhancement of maritime security," and Resolution 10 for "early implementation of long range ship's identification and tracking (LRIT)." A time line indicating various initiatives leading to the development of LRIT and the current piracy related activities is shown in Fig. 2.

Conceptualising LRIT

During the 81st Session of Maritime Security Committee, held at IMO Headquarters in London on May 10-19, 2006 regulations for LRIT were included in the SOLAS Chapter V on Safety of Navigation. LRIT was made a mandatory requirement with effect from December 31, 2008 for merchant ships (over 300 gross registered tonnage (GRT)) on international voyages and mobile offshore drilling units. The system envisaged automatic transmission of position data by ships every six hours, as a structured message for subsequent dissemination to contracting nations. Thus, while LRIT position updates were not continuous, the transmissions were to be made to the designated data centres and not directly to port(s) or coastal state(s). The users would receive information through their nominated data centre via a system of international data exchange (IDE) and previously mandated data distribution plan (DDP). Thus, a nation could specify the frequency of reports and ranges desired, and also lay down restrictions if it wanted to deny the data to any country. Further, search and rescue (SAR) services of contracting government were envisaged to receive free LRIT information in relation to SAR of persons in distress at sea. A schematic diagram of LRIT system is shown in Fig. 3. Though the proposal for LRIT implementation has been taken up for discussion at IMO on a number of occasions, consensus could not be achieved on two issues. The first relates to access of LRIT information irrespective of location. The second pertains to the need for establishing the tracking distance or period. Concerns have also been aired about the vulnerability of shipping data held with the data centres.

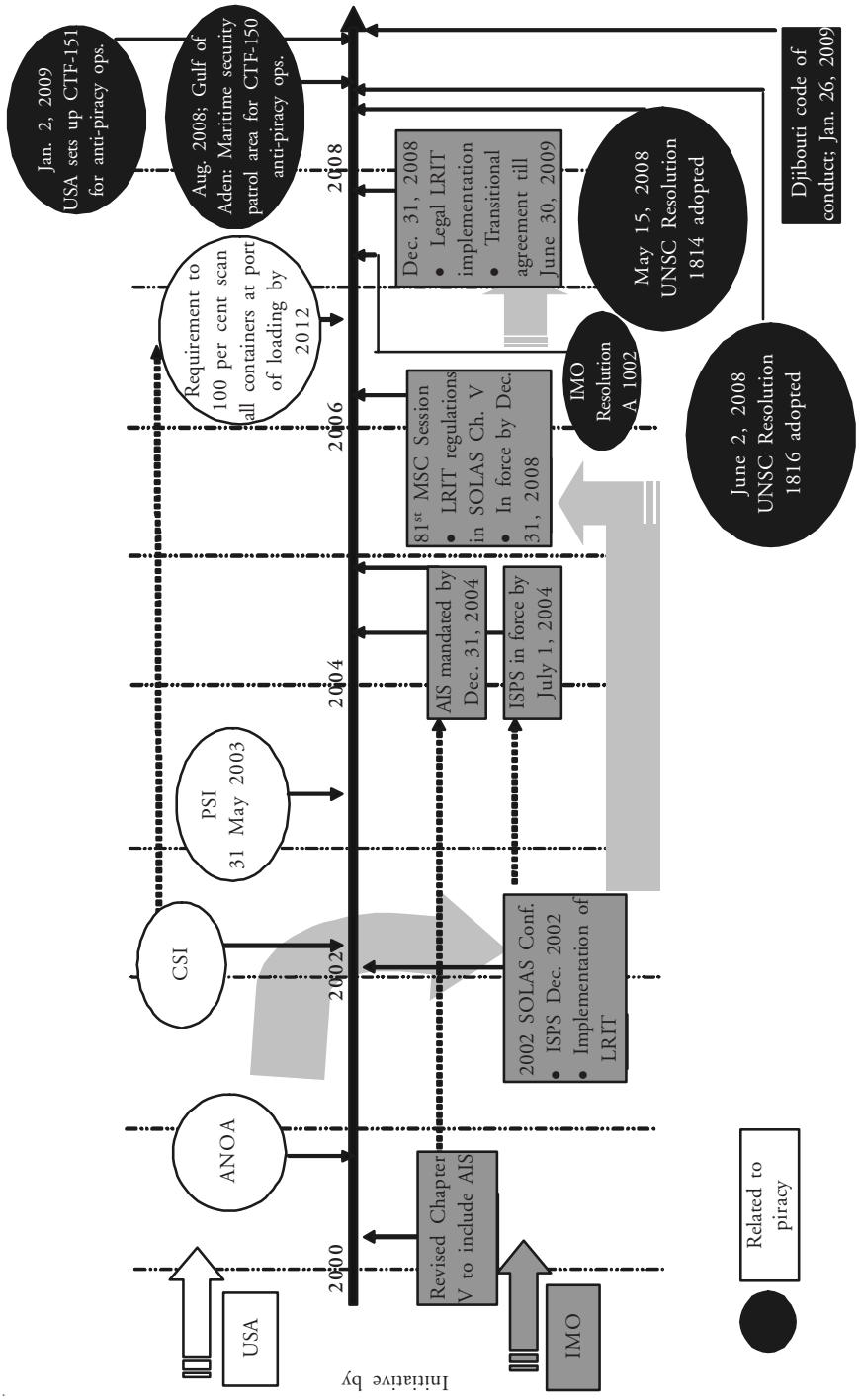

Fig. 2. A timeline towards maritime security.

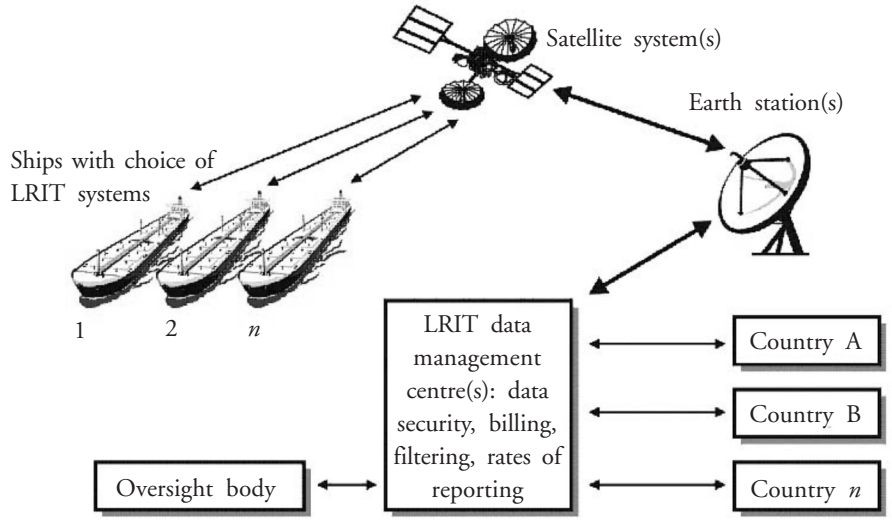

Fig. 3. LRIT system details; Source: Cairns, B., AIS/06, October 10-11, 2006, Office of Navigation Systems, US Coast Guard.

During deliberations, the US proposed 2,000 nm distance from the coast as the control area for tracking movement of ships, which is consistent with its policy of ANOA of 96 hours at an average speed of 20 knots. However, a large number of members, including China, recommended 200 nm, as provisioned in the United Nations Convention on the Law of the Sea (UNCLOS) to ensure freedom of navigation. It may be understood that the UNCLOS authorises national jurisdiction up to 200 nm, but it does not actually forbid tracking of vessels beyond this limit. The LRIT information envisages to only include the ship's identity, her location and the destination port. Importantly, warships are not required to comply with LRIT stipulations. The following factors could dictate the limit for tracking distance from a coastal state:

- The geographical location of the country and its proximity to other nations;
- Areas of sea interest;
- Proximity to shipping lanes and choke points;
- Threat perceptions;
- Response time, including organisational set-up and response capabilities, in terms of ship-borne and airborne surveillance resources; and
- Cost implications.

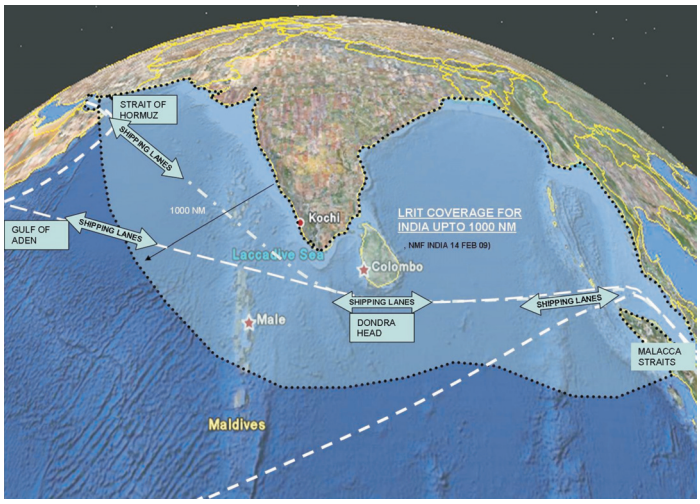

Fig. 4. LRIT coverage.

LRIT Positional Data: Limiting Distance

The choke points that envelope India's strategic area of interest are Bab-el-Mandeb (1,300 nm) and Strait of Hormuz (950 nm) to the West, Cape of Good Hope to the South and Malacca Strait (1,313 nm) to the East. In addition, very busy sea lanes pass close to the mainland with heavy traffic density (Fig. 4). On an average, around 1,200 ships are present each day within 1,000 nm of the Indian coast. The International Maritime Bureau (IMB), Kuala Lumpur recognises Malacca Strait and the Somalia Coast as "hot spots" on the piracy and maritime terrorism map, that pose additional security concerns. It would be essential to have real time data on all vessels entering India's area of interest through these choke points. As the density of traffic through these choke points is very high, a credible reaction time is required to evaluate threat perceptions and validation. Thus, it was prudent to source positional report up to 1,000 nm from the Indian coastline.

In subsequent deliberations at IMO, the Council mandated that SOLAS contracting governments will be entitled to receive information about ships navigating within a distance not exceeding 1,000 nm off their coast. In light of divergent views held, the 81st Session resorted to a conciliatory measure by adopting this limit. However, the limit meets India's concerns. The regulation foresaw a phased-in implementation schedule for ships constructed before its expected "entry into force" date of January 1, 2009. It also identifies the authorities that may have access to LRIT information. Also, no interface is envisaged between LRIT and AIS.

Under LRIT, nations can source positional reports in three capacities viz. Flag State, Port State and Coastal State. As a Port State, a nation is entitled to receive position data from the time a ship makes its intent to visit the port, irrespective of the 1,000 nm limit. LRIT information would be provided to contracting governments and SAR services, upon request, through a system of national, regional, cooperative and international LRIT data centres. Each nation would provide to the selected LRIT data centre a list of the ships entitled to fly its flag, which would be required to transmit LRIT information. These ships would transmit LRIT information data, only to the LRIT data centre designated by authorities. However, it maintains the right of a Flag State to protect information about the ships entitled to fly its flag, where appropriate, while allowing a Coastal State access to information about ships navigating off its coast(s).

LRIT Initiative: Key Issues

Safety or Security?

From the very beginning, nations objected to the concept of LRIT – largely seen as IMO's recognition of ANOA (US initiative). There was reluctance by some states to put any imposition on ships with regard to provision of positional updates. Access to positional information of ships employed on trade was seen widely as inimical to economic well being. A large share of the world shipping tonnage is held or registered with countries that offer a FoC. This provides considerable leeway and concessions to the shipping companies and such countries get a source of additional revenue. The necessity of LRIT was perceived by the shipping fraternity as a requirement for addressing the security issues of Coastal States and not as a safety requirement for ships, like AIS.

Financial Viability

The cost implication of putting in place such system was a major bone of contention. During the deliberations at IMO, entities with greater shipping tonnage argued, with success, that the cost for LRIT should be borne by the state and not the shipping fraternity. Hence, the cost for transmissions of position reports by ships were to be borne by the Flag States. The financial implications, thus, were clearly on setting up of the data centres, cost of transmission of reports and on the cost of each report sought. It was estimated that if four reports were sought by a nation, the average cost per report could be in the region of US$ 0.25. The data centres would be the

transiting hubs for sourcing report as well as billing. For example, if India demanded report of all ships with 1,000 nm, then data of all ships present within the envelope would be sourced from different data centres and made available to India's data centre. Subsequently, the respective data centre would forward billing charges to India's data centre. Thus, if reports sought from a particular data centre were low, keeping overhead running costs constant, the cost of the report sought would be higher. Further, the cost for the IDE, the logic for ensuring flow of data between data centres, and the LRIT Coordinator also needed to be shared. This put severe constraints on the financial viability of the data centre and thereby on the implementation of LRIT. However, with constant US support, the implementation of LRIT has continued. In fact, the US had also offered to host and operate both the IDE as well as an International Data Centre[19] (for countries that do not wish to set up a data centre or partake in a cooperative data centre), on *gratis* terms till alternate arrangements are put in place. The US offer for the IDC was viewed with suspicion by many nations which believed that the data would be resident with the US and could be used for other purposes.

Choice of Data Centre

A number of countries such as the US, Russia, Marshall Island etc., have set up National Data Centers.[20] Some others such as the European Union (EU)[21] have gone ahead and set up a Regional Data Center. Due to cost implications and the perceived irrelevance of LRIT, many nations have decided against setting up a data centre and have opted for a cooperative data centre. India has decided to set up a National Data Centre uner Directorate General of Shipping (DGS) at Mumbai with the assistance of M/s Antrix/Indian Space Research Organisation (ISRO). The DGS is also the nodal agency in India for LRIT. The other stakeholders include maritime enforcement agencies, shipping companies and port authorities (Fig. 5). The application service provider is M/s CMC Ltd., the communication service provider is M/s Tata Communications.

Meeting Implementation Deadline

Though the deadline of December 31, 2008 has elapsed, the implementation of LRIT could not be executed due to lack of conformity by all contracting nations. International Mobile Satellite Organisation (IMSO),[22] the LRIT Coordinator,[23] is still grappling with the task of setting up the IDE and DDP. Therefore, in December 2008, IMO agreed to transitional arrangements until June 30, 2009, following legal implementation on

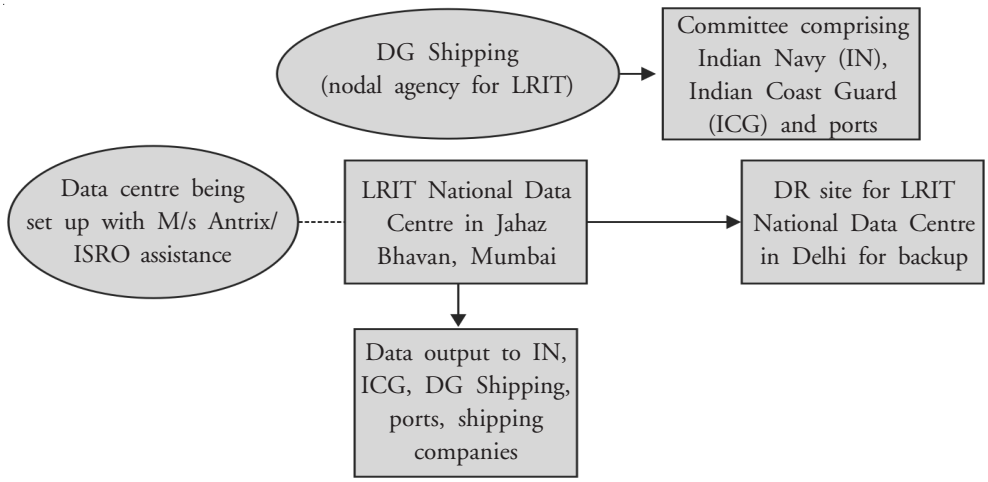

Fig. 5. LRIT implementation in India.

December 31, 2008. However, the US, amongst others, has advised IMO that after June 30, 2009, ships could be detained if their Flag State has not fully implemented LRIT.[24] International Chamber of Shipping (ICS) has stressed to governments that imposing sanctions against shipping for non-compliance with LRIT measures that are the responsibility of state administrations, and beyond the control of ships, would be inappropriate and unacceptable.

A Sub-Continental Regional Data Centre

Though India has indicated its intent to IMO to set up a National Data Centre, it might be prudent in the country's interest to expand it to a Regional Data Centre. It may be of some interest to note that participation of South Asian countries at the IMO deliberations, particularly the Arabian Sea and Bay of Bengal littorals has been minimal. The cold response could be attributed, primarily, to the cost factor as well as technological issues and threat perception. Further, neither of these countries has a sizeable merchant marine that would make them a key player. Expanding the National Data Centre to a Regional one augurs well both for India and the littoral countries. In fact, the services could be offered on "only use" basis thereby reducing cost implications and, thus, enhance acceptance. Hence, there is a need to proactively pursue diplomatically and gain consensus for a Regional Data Centre, which could also include countries on the fringe such as Oman, Kenya, Mauritius etc. In the larger sense it would ensure larger

domain awareness at significantly lesser cost implications. This would also pave the way for larger participation in India's other initiative of developing coastal security framework such as national AIS Network, tracking mechanism for minor crafts etc. This could be taken on the Indian Ocean Naval Symposium forum for ascertaining consensus.

Cost Implications

Although it has been said that cost should not be a limiting factor when addressing security, one needs to factor in the running cost of LRIT. Leaving aside the initial capital that is required for setting up LRIT infrastructure, the major running cost would arise from the reports being sought. It is, therefore, necessary to estimate the number of reports that are likely to be sourced to arrive at the cost implication. The stakeholders that are likely to source the LRIT reports would include Indian Navy, Indian Coast Guard, Marine Police and Port Authorities. Ports have been mandated to receive position reports in accordance with received Notice of Arrival beyond the prescribed limit, once a ship conveys its intention. LRIT requires ships to provide four position reports daily, commencing at 0000 hrs GMT. For sake of simplicity, one could divide the zone of 1,000 nm into two distinct areas with respect to the frequency of reports that are sought and the extant demarcated responsibilities. For a zone from 1,000 to 350 nm off the coast, it may suffice to seek two position reports every 24 hours (say 0000 and 1200 hrs GMT). On an average speed of 20 knots, a ship would traverse 240 nm before the next report is received. Thus, if a ship was just beyond 1,050 nm at 0000 hrs GMT, its position will not be reported. However, in the next 12 hours, it would be about 800 nm from the coast, which is the "worst case" scenario. Within 350 nm (limit of the continental shelf), four position reports, that is a report every six hours should be considered mandatory. A frequent reporting may not accrue any additional benefit. It needs to be borne in mind that a country can seek more frequent report if it desires by submitting a request. It can also demarcate an area for seeking more frequent reports. An estimate puts about 800 ships within the 350 nm limit and about 1,200 ships within the 1,000 nm off India's coastline at any given time. These estimate have been drawn from various figures for the transit routes at India's maritime extremities. Though the figures vary, a rough estimate at US$ 0.25 per report would mean incurring expenditure of US$ 219,000 (1,200 × 2 × 365 × 0.25) for seeking two reports within 1,000 nm, or US$ 292,000 (800 × 4 × 365 × 0.25) for seeking four reports within 350 nm. Various agencies have sought to increase

the frequency of reporting within 50 nm from the coast. However, it may be prudent to address the issue with other measures such as National AIS Network and Coastal Radar Chain. The need to seek more frequent report on a ship that has been tracked through 1,000 nm needs to be pragmatically thought about.

LRIT Positional Data

Handling Data

One also needs to consider the proposed processing of the data gathered once the system is established and running. On an average, approximately 4,000 reports daily or about 1,460,000 reports annually would be generated. The gravity of the situation can be assessed from the fact that these concern only ships under the ambit of the LRIT. Obtaining data is just the input to establishing any kind of domain awareness. In reality, more importance would have to be given to the collation, analysis and, thereafter, dissemination of this data. The date processing would result in trend analysis, which would generate immense data on traffic pattern. This pattern when suitably dovetailed into the system would provide easy correlation on non-compliance and suspicious movements. This task would require a dedicated team of professionals drawn from various stakeholders to provide homogeneity of effort. It would also make sense to outsource the task as it does not necessarily involve maritime expertise. Unless this aspect of processing is factored in, the LRIT position data would just be confined to archives with no meaningful result.

Data Implications

We now look at another related issue that LRIT positional data may have an effect on. It is a known fact that merchant marine are reluctant to participate in LRIT owing to so-called fear of compromising on trade competitiveness. However, a more serious implication would be "trade warfare", which has been an important tool in any conflict as it affects the war waging ability of a nation. In a high-intensity conflict at sea, the failure to safeguard maritime trade will have adverse consequences and critical implications on the war's outcome, like the disruption of North Atlantic trade by German U-boats during World War II. Maritime forces, world over, whilst practicing trade warfare to disrupt the adversary also ensure continuity and safety of own trade through naval control of shipping.

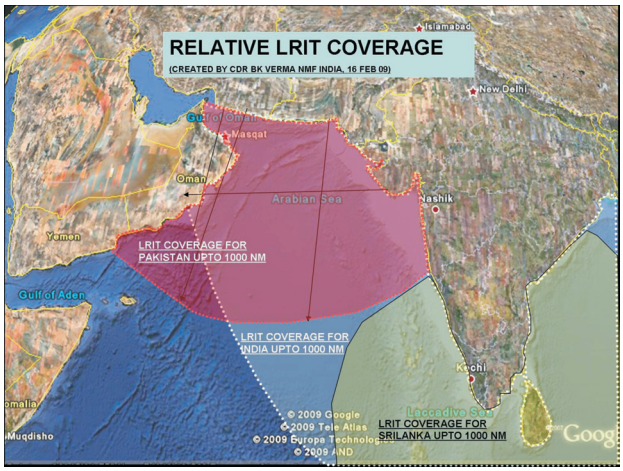

Fig. 6. Relative LRIT coverage.

Maritime Trade Imperatives

Not only would LRIT enhance MDA it would also provide immense inputs on the pattern and criticality of trade supplies. It cannot be denied that availability of shipping route data, specifically in littoral warfare, could be effectively exploited for trade warfare. In the case of India, a 1,000 nm coverage to Pakistan would provide the latter with information of all vessels till a latitude South of Mumbai (Fig. 6). This envelope encompasses the Gulf of Kutch and the ports of Mumbai and JNPT, which account for a significant portion of critical trade for India. Similarly, India would have input on all ships transiting in the Northern Arabian Sea encompassing the entire Makran coast. With this kind of domain awareness, the existing concepts of protection of merchant marine would need re-evaluation. One of the key pre-requisites for success in defence and protection of maritime trade in times of war is the availability of a sound and fully-tested doctrine. One cannot afford to permit an adversary to disrupt the global supply chain by attempting to block vital sea lanes of communications and commerce.

Looking Ahead

It suffices to say that the world economic trade literally moves on the ocean and will continue to do so. It is important to realise the gravity of the threat of maritime terrorism and piracy, as prevalent today. During the past few years, a number of initiatives have been taken towards improving and defining the maritime security

environment. These issues have been accorded 'primacy' only due to the perceived threat of maritime terrorism and piracy. The initiatives have been directed towards processing and managing a "recognisable maritime picture" to enhance the security environment for day-to-day operations. It is all too apparent that the LRIT initiative is, literally, a development over the USCG ANOA and is being primarily driven by the US, yet, one should look at the benefits that could accrue. The availability of data on merchant traffic justifiably raises concerns wherein the same could be used by adversaries to target a nation economically. However, the LRIT initiative and the issue of data security need to be evaluated in light of the present concerns of the world. What needs to be analysed is the advantages of such initiative in enhancing maritime security against terrorism and piracy as against the disadvantages of such data falling in the hand of an adversary and, in times of war, the same being used to target the nation economically. The operational implications are more deep rooted than what is apparent. There is a need to review India's operational tactics to address the challenges, thus, posed.

There have been hurdles in pursuing the LRIT initiative, which is also threatened by the technological advances in the recent past. The AIS, being V/UHF based, has been exploited within its restriction for coastal surveillance through institution of Coastal AIS Networks. In the recent past efforts have been made to capture the AIS signatures using a low Earth satellite (LES), which has a low orbital period and provides periodicity of approximately 2 to 3 hours. A Canadian firm, M/s COM DEV International Ltd.[25] is carrying out development work in the area of MDA. In April 2008, the firm placed a payload on the Polar Satellite Launch Vehicle launched from Sriharikota. The payload is successfully capturing the AIS signatures of vessels in its orbital footprint and transmitting back at intervals of about 2 to 3 hours. In a press release, the firm stated that it had validated the advanced space-based AIS performance capability that it has developed.[26] In fact, the firm plans to place several of such payloads on various satellites being launched to cover the globe. The firm has also been awarded a contract worth US$ 8.6 million to design, build and launch a micro-satellite for the Government of Canada. The Maritime Monitoring and Messaging Micro-satellite (M3MSat) is a technology demonstration mission that will be launched in 2010.[27] M3MSat is expected to demonstrate the full capability of advanced spaced-based AIS technology developed by COM DEV. This initiative *prima facie* appears to provide faster positional updates with significant lesser cost implications. Therefore, it could possibly also threaten the concept of LRIT and, thus, needs to be evaluated.

As India is at the threshold of entering a LRIT enabled maritime awareness domain, it would be prudent to put in place procedures and infrastructure that would maximise the data received. The DG Shipping, in partnership with the Indian Navy and Indian Coast Guard, is setting up the infrastructure with assistance of M/s Antrix Corporation Ltd. These agencies would need to work jointly to enhance the overall effectiveness of LRIT and the resultant MDA through the following:

- A joint mechanism comprising DG Shipping, Indian Navy and Indian Coast Guard to coordinate and manage the LRIT;
- A separate and dedicated body to effectively address the data management issues and an analysis body through scientifically derived procedures;
- Integration of LRIT into the coastal surveillance schemes (radar and AIS chain) to arrive at a seamless recognised picture;
- Rational approach, through sharing, towards meeting the expenditure incurred;
- Discourage individualistic attempt at LRIT utilisation; and
- Re-evaluating the concept of trade warfare and naval control of shipping.

Notes

1. United Nations Conference on Trade and Development (UNCTAD) estimates that the operation of merchant ships contributes about US$ 380 billion in freight rates within the global economy, which is equivalent to about 5 per cent of total world trade, www.marisec.org/shippingfacts/worldtrade (accessed January 27, 2009).
2. Value of volume of world trade by sea, www.marisec.org/shippingfacts/worldtrade (accessed January 27, 2009).
3. World Oil Transit Chokepoints, www.eia.doe.gov/cabs (accessed January 20, 2009).
4. Donna J. Nincic, Sea Lane Security and US Maritime Trade: Choke Point as Scare Resources, Chapter 8, Globalisation and Maritime Power 2002, Institute for Strategic Studies, National Defence University, www.ndu.edu (accessed January 12, 2009).
5. AIS Transponders, www.imo.org (accessed January 03, 2009).
6. Norwegian AIS Network: Status and Operational Use, HELCOM AIS EWG 9/2005, Tom Braute and Terje Alling, Norwegian Coastal Administration, www.fargisinfo.com/hits/LinkedDocuments/NorwegianAIS_Helcom.pdf (accessed December 27, 2008).
7. Year End Review 2008, Press release of the Department of Shipping, Ministry of Shipping, Road Transport and Highways, Government of India, New Delhi, December 29, 2008 http://pibmumbai.gov.in (accessed January 14, 2009).

8. *Ibid*.
9. USCG National Vessel Monitor Centre, www.nvmc.uscg.gov/nvmc (accessed January 14, 2009).
10. Container Security Initiative, www.cbp.gov/xp/cgov/trade/cargo_security/csi (accessed January 23, 2009).
11. Container Security Initiative: Is India Serious About Its Maritime Trade?, Vijay Sakhuja, Observer Research Foundation, New Delhi, www.ipcs.org/article_details.php?articleNo=1748 (accessed January 23, 2009).
12. Container Security Initiative, http://worldtraderef.com (accessed January 23, 2009).
13. India and US-led WMD Non-Proliferation Initiatives, Amit Kumar, Observer Research Foundation, www.pugwashindia.org (accessed January 24, 2009).
14. Key Issues: Year in Review 2008, 100 per cent Container Scanning, www.marisec.org/ics-isfkeyissues (accessed January 27, 2009).
15. India to Join Global Container Security Initiative, The Hindustan Times, June 24, 2007 (accessed January 27, 2009).
16. Proliferation Security Initiative, Sharon Squassoni, September 14, 2006, CRS Report RS21881 for Congress, http://ftp.fas.org/sgp/crs/nuke/RS21881.pdf (accessed January 29, 2009).
17. International Convention for the Safety of Life at Sea (SOLAS), 1974, www.imo.org (accessed January 20, 2009).
18. Maritime Security, www.imo.org (accessed January 20, 2009).
19. Para 5, Guidance on Implementation of LRIT IMO MSC Circular MSC.1/Circ 1298 dated December 8, 2008, www.imo.org (accessed January 20, 2009).
20. LRIT, http://en.wikipedia.org/wiki/Long_Range_Identification_and_Tracking (accessed January 20, 2009).
21. EU LRIT System and Data Centre, https://extranet.emsa.europa.eu; also, EMSA Selects CLS to Deliver European LRIT Data Centre, www.cls.fr/documents/solutions/maritime/news/2008-11-06_press_release_EMSA-LRIT-CLS_en.pdf (accessed January 20, 2009).
22. The International Mobile Satellite Organisation (IMSO) is an inter-governmental organisation that oversees certain public satellite safety and security communication services provided via the INMARSAT satellites.
23. LRIT Coordinator, www.imso.org/whatisimso_UK.asp (accessed January 20, 2009).
24. International Shipping Federation Monthly Newsletter January 2009, www.marisec.org/news/index.htm (accessed January 20, 2009).
25. www.comdevintl.com (accessed January 20, 2009).
26. *Ibid*.
27. COM DEV Awarded AIS Micro-Satellite Contract with Canadian Government, www.gisdevelopment.net/news (accessed January 20, 2009).