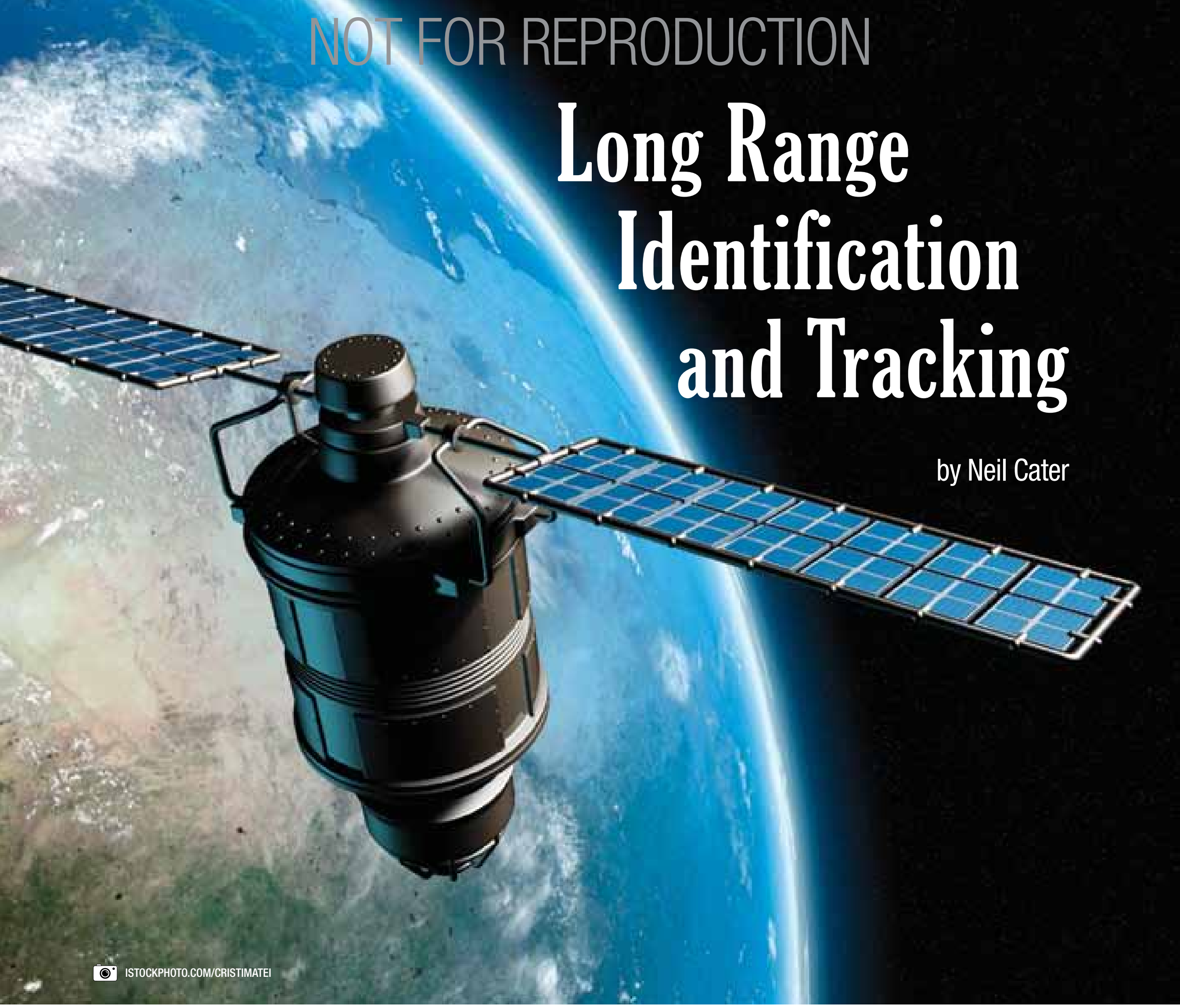
Long Range Identification and Tracking

by Neil Cater



ISTOCKPHOTO.COM/CRISTIMATEI

Introduction

Matters relating to ship borne acts of aggression and the security of ships and their crews have long been a concern to maritime interests. Since the onset of the age of exploration, fleets of vessels have fought for control of waterways. With the advent of international sea trading routes, there came the arrival of marauding pirate ships. The technology behind the weapons of aggression as well as that behind the corresponding tools of awareness and avoidance have evolved over the centuries since man first took to the oceans on military or commercial ventures. For most of this time, the element of surprise and the tactical advantage this brings has rested firmly with the aggressor. The invention and refinement in the last century of wireless radio and radar technologies offered the tools to communicate with and detect vessels of interest beyond human line of site. In reality, both of these technologies have had a profound effect on marine transportation in that each has done its part to increase the area of maritime domain awareness.

Even with the technological advances of the last century, two issues in particular continue to limit the effectiveness of maritime domain awareness. First is the selectivity and size of the zones. Our oceans cover a vast area and our ability to provide effective surveillance is limited. Even with the best ship and shore based technologies, coverage is limited to little more than a hundred nautical miles, often in narrow sectors ***... Is there really no-one out there, or are we just looking in the wrong places?*** A second concern regards the ability to positively track and identify vessels of interest. In other words, those responsible for ship and port security must be confident that once a vessel or a target of interest has been identified there is a means of maintaining a unique file on that target until the vessel either docks or ceases to become a vessel of interest. This is a particular concern in obstructed and congested bodies of water.

Two incidents of maritime terrorism that occurred around the time of the September 11, 2001, terrorist attacks in the United States served to focus the resolve of the maritime community to answer the threat of terrorism with enhanced maritime security. The first incident, the bombing of the *USS Cole*, preceded the events of September 11, 2001, and had already served to focus concerns of imminent attacks on major maritime assets by the time of the attacks in the United States. On October 12, 2000, the *USS Cole*, an Arleigh-Burke class Navy destroyer, was on a routine refueling stop in the port of Aden, Yemen, when a small craft loaded with explosives and piloted by two suicide terrorists was detonated along side. The resulting explosion killed 17 US servicemen, injured 37 others, and caused $250 million in damage to the ship. Nearly two years later, on October 6, 2002, the French tanker, *Limburg*, exploded off the coast of Yemen with considerable environmental damage resulting from the oil spill created by the incident. Investigation into the incident confirmed fears that the explosion was an act of terrorism, allegedly initiated again by a small high speed vessel piloted by suicide bombers.

The immediate response in the aftermath to these disturbingly similar events was the development of a framework by the International Maritime Organization (IMO) for the creation of the International Ship and Port Facility Security (ISPS) Code. Measures that have been adopted within the ISPS code include Regulation 6 that mandates the requirement for ship's safety alert systems, introduced in 2004. The ISPS Code also called for the adoption of Long Range Identification and Tracking (LRIT) as a matter of priority.

A Brief History of LRIT

The IMO was established by convention in 1948 and first met as an organization in 1959. Headquartered in the United Kingdom, it operates as a special agency of the United Nations and represents 168 member states and three associate members. The overall mission of the IMO is to develop and maintain a regulatory framework governing all aspects of shipping engaged in international trade. Operating as a series of conventions, IMO work falls primarily into three categories: safety of life, prevention of marine pollution, and liability and compensation.

When the IMO came into existence, a number of important maritime conventions, most notably the 1948 Safety of Life at Sea (SOLAS) convention and the 1954 International Convention on the Prevention of Pollution at Sea by Oil, were already in force. IMO was given responsibility for the maintenance of these and other existing conventions as well as the development and adoption of new conventions as the need is indentified.

Regulations are developed and amended through participation in technical committees consisting of expert representatives of member states. The drafting, approval, and subsequent adoption of a convention can, depending on the nature of the work, be a very long and arduous process, often spanning several years from initial identification to the ultimate adoption by IMO. Following adoption by IMO, a convention must then be individually approved by the member countries before it is observed and enforced. Where there is an identified requirement to address emergency or otherwise high priority circumstances, member states can agree to accelerate this process and fast track the ratification and adoption of a convention. Such is the case we have witnessed in the development and adoption of the ISPS code and its subsequent recommendations regarding Ship's Security Alerts and Long Range Tracking and Identification of ships.

In May 2006, the IMO Maritime Safety Committee adopted Resolution MSC.202(81), an amendment to the SOLAS convention, enabling contracting governments to undertake the long range tracking and identification of ships. The information requirements are basic and include a ship's identity, its position, and a time and date stamp. On January 7, 2008, Regulation 19-1 was brought into force with a mandatory compliance date of December 31, 2008. Resolution MSC.202(81) applies to all passenger vessels including high speed passenger craft, all cargo ships greater than 300 GRT, and all Mobile Offshore Drilling Units that are engaged in international voyages. The capability for LRIT is a mandatory fitment on all new vessels built after December 31, 2008, and upon the event of the first radio inspection after December 31, 2008, on existing vessels in these classes.

Coincident with the adoption of MSC.202(81), the Maritime Safety Committee also adopted Resolution MSC.211(81) prescribing arrangements for the timely establishment of LRIT. This resolution recognized the need for an expedited implementation of LRIT. Contracting governments to the SOLAS convention were asked to advise the Maritime Safety Committee of its plans to establish national and regional LRIT data centres. As well, contracting governments were asked to submit proposals regarding the establishment of an international LRIT Data Centre and Data Exchange. The International LRIT Data Centre was to be operational by July 1, 2008, with national and regional centres to follow by October 1, 2008.

Figure 1: The IMO Maritime Safety Committee Resolution on LRIT applies to passenger vessels, cargo ships, and Mobile Offshore Drilling Units. Here a passenger ferry navigates the waters off Vancouver Island, British Columbia.

Figure 2: Container terminal in Germany.

ISTOCKPHOTO.COM/PIXELPROF

The International LRIT Data Exchange and Data Centre

Subsequent to resolution MSC.211(81), the Maritime Safety Committee, in May 2008, adopted SC.264(84) accepting a proposal from the United States to establish an interim international LRIT Data Exchange until such time as a permanent International Data Centre can be established. This step was essential in ensuring that the data exchange capability was up and operational at the time of the mandatory compliance date of December 31, 2008.

The single most important element of the LRIT system architecture is the International Data Exchange. Briefly, the International Data Exchange is connected to all LRIT data centres worldwide, and handles the routing of data between national and regional data centres. LRIT information is considered critical in nature and consequently every step is taken to ensure there is no loss or corruption of data during the exchange process. All transactions between data centres employ a store and forward buffer to ensure the integrity of data. All LRIT data transactions are maintained in a traffic record for a minimum of one year. This record of archived data is used primarily as a means of record for invoicing and settlement between contracting governments and data centres. Archived data is also available for audit purposes.

The overall functionality of the LRIT network is defined by the LRIT distribution plan. The first feature of the distribution plan is a listing of all entities that are entitled to exchange LRIT information. This list includes, of course, the international, regional, and national data centres and additionally includes all contracting governments, search and rescue agencies as well as other LRIT data users such as application service providers (ASPs) and communications service providers (CSPs).

Figure 3: Coastal ferry entering Oban, Scotland.

For each contracting government, the LRIT distribution plan maintains a profile that governs its privileges and preferences for operation within the international network. A key piece of the profile is the definition of its territorial waters in accordance with applicable international law. Within these territorial limits, the distribution plan maintains a list of all ports, facilities, and other destinations under the authority of the contracting government including a list of locations, by co-ordinates, that ships for which LRIT is mandatory may enter or proceed to as is appropriate. Not all contracting governments may, for defense and security or for commercial reasons, wish to have information regarding vessels flying its flag released to a particular administration. Recognizing this reality, the LRIT distribution plan makes provision to exclude an authority from receiving LRIT information from vessels flying under a particular flag.

LRIT information must by its nature be reliable safe and secure. The consequences of data that are lost, corrupted, or misdirected during exchange defeat the primary reason for the LRIT program. System security is based on four guiding principles: authorization, authentication, confidentiality, and integrity. First, the ability to receive and view specific LRIT information should only be granted to those so authorized. Second, parties exchanging LRIT information require an authentication. Third, confidentiality of the LRIT information is maintained on the application server to ensure that the content is not inadvertently disclosed during exchange. Finally, the integrity of the information must be upheld to ensure that no data has been altered.

LRIT reports are initiated in two ways: scheduled reports that are automatically transmitted from a vessel and on-demand reports that are requested by the data end user. Latency is defined as the time elapsed between when a LRIT report is either automatically transmitted or requested by the user and when the report is available to the end user. In the case of scheduled reports, the maximum acceptable latency is 15 minutes; for on-demand reports, the maximum latency is 30 minutes. The system performance specification stipulates that the maximum latency specification be met 99% of the time over any month and 95% of the time over any 24-hour period.

Responsibilities of Contracting Governments and Administrations

The Maritime Administration, or simply the administration of a contracting government, is normally the national department or agency that is responsible for the safety of ships, the protection of life and property at sea as well as being responsible for the enforcement of all applicable laws and regulations. This would typically be the Coast Guard or the National Marine Transportation Agency.

Each maritime administration must first establish which national or regional LRIT data centre that mandated vessels sailing under its flag must report through. For each mandated vessel, the administration must provide to its LRIT data centre basic information consisting of the ship's name, its IMO number, its radio call sign, and its Maritime Mobile Service Identity. If a vessel is permanently taken out of active service, it is the responsibility of the administration to notify the LRIT data centre of the details as well as the date and time of the change of status. When a vessel is transferred or sold to another flag state, it is the responsibility of the new administration to notify its data centre of the particulars of the new vessel.

Each contracting government must recognize and respect the importance of LRIT information that it is entitled to receive. First and foremost, the information must be used for purposes that are consistent with international law. Much of the LRIT information that comes into the possession of a contracting government is commercially sensitive in nature and therefore must be protected from unnecessary or unauthorized distribution to third parties. In circumstances where a contracting government has security concerns regarding the release of information to another contracting government,

Figure 4: Lifting a container from a stack to a ship.

it is entitled to stop the distribution of LRIT information transmitted from ships that are entitled to fly its flag.

Distribution of LRIT information is, under most circumstances, based on a user pay model. A contracting government is responsible for costs associated with acquiring any LRIT information that it requests and cannot charge ships for information that they request. Likewise, a ship is not responsible for costs associated with transmitting LRIT information to its home administration. In the event that LRIT information is requested by a search and rescue organization in relation to the distress of persons at sea, this information is provided free of charge.

The requirement for vessels, depending on classification, sizes and nature of business, to transmit LRIT information is mandated by IMO SOLAS Regulation 19-1. Once LRIT information is received by the appropriate data centre, it is archived and maintained for a minimum of one year. During this period, contracting governments have authority as to when and how to responsibly use long range identification and tracking information that it is entitled to receive under the terms of Regulation 19-1. There are essentially three distinct circumstances where a contracting government is entitled to receive LRIT information for security and traffic management applications:

- All mandated ships that are entitled to fly the flag of the contracting government wherever they are located.
- All mandated ships that intend to enter a port or facility that is under the jurisdiction of the contracting government.
- All mandated ships that do not intend to enter a port or facility of a contracting government but intend to navigate within 1000 nautical miles of its coast.

Vessel Data Reporting

Care has been taken in the implementation of LRIT to ensure that the cost and operational burden on ships and ship owners is as little as possible. This is perhaps best seen in the acceptance of the Inmarsat C and Mini C satellite communications services as the first communications medium for LRIT. Inmarsat C and Mini C are, first and foremost, highly reliable and globally available store-and-forward-type satellite data services. The up-front costs for the shipboard terminals is relatively low and the service pricing model, which is based on the volume of data transmitted, is ideally suited to the LRIT application where the traffic consists of small periodic bursts of data.

Furthermore, with few exceptions, all ships for which LRIT is mandated must also comply with the terms of the global maritime distress and safety system (GMDSS). Inmarsat C is one of a number of common services used to meet GMDSS compliance and is consequently already available on most vessels that must comply with LRIT regulations. Because of the near worldwide availability and acceptance of Inmarsat C and Mini C, there is a global network of communications and applications service providers (CSPs and ASPs) that offer end-to-end integration and delivery of Inmarsat C data services.

Service providers provide the continuity in the network between the vessels and their authorized LRIT data centre, provide transaction management, and ensure that information is stored and routed in a secure accountable manner. To keep reporting costs to an absolute minimum, only a minimal information packet is transmitted from a vessel over the Inmarsat C satellite link. Consequently all that is typically transmitted from the ship is its position, the time and date that the position was provided, and a unique identification number. The service provider, through the course of handling the information, adds value at a number of points. First, the Inmarsat identification number, while unique to a vessel, does not in and of itself identify that vessel. Consequently the service

Figure 5: The ISPS Code called for the adoption of Long Range Identification and Tracking (LRIT) as a matter of priority. Here a ship's mast holds communication and location equipment.

provider will add other information on the vessel including the IMO ship's identification number and the plain language name of the vessel. The integrity and traceability of LRIT information is paramount to achieving the objectives of the program. The service provider adds additional timestamps to the LRIT message at each point as it is routed through the network from the point it is retrieved from the Inmarsat system until it is ultimately delivered to the data user.

A typical Inmarsat C service provider can remotely integrate and connect shipboard equipment to the LRIT data centre and can perform control and configuration of the LRIT data transmitted from a ship. For example, depending on the nature of operations or the waters being sailed through, a ship may be required to change the interval of or suspend the transmission of LRIT information or to transmit information on demand.

Future Implementation of LRIT

At the initial IMO MSC meeting regarding LRIT in May 2006, the need for a timely and orderly roll-out of LRIT was recognized. To ensure early adoption and reliance on LRIT by the maritime community, a communications medium was required with the reliability and ubiquity to ensure that it would essentially be a risk-free element as the service was established. Consequently, implementation and operation of LRIT to date has relied on the Inmarsat C and Mini C services as the communications medium for reporting LRIT information. However, IMO Resolution MSC.263(84), "Revised Performance Standards and Functional Requirements for the Long Range Identification and Tracking of Ships," does not stipulate specific communications service for the vessel to shore reporting requirements.

Figure 6: A container ship entering Swan River, Freemantle Port, Western Australia. Care has been taken in the implementation of LRIT to ensure minimal costs for ship owners.

Figure 7: Communication and safety equipment onboard a yacht.

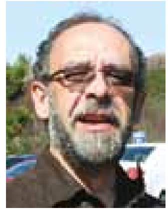
Early in 2009, Iridium Satellite LLC announced that it had begun certification of service providers to offer LRIT services over the Iridium satellite network. The Iridium LRIT performance standard is based on the Iridium short burst message. While Inmarsat C is, in most cases, ideally suited to the LRIT application, the service is offered only over a geostationary satellite constellation. Geostationary satellites are held in a fixed location over the equator and offer constant coverage of a particular area of the earth's surface. The distribution of the 11 Inmarsat satellites around the globe approximately 36,000 km above the equator provides continuous coverage of the globe between the 70 degrees north latitude and 70 degrees south latitude. Consequently, while the Inmarsat constellation does offer the required capacity and reliability over most of the globe, vessels that operate north or south of the 70th parallels cannot use Inmarsat services to meet their LRIT obligations because the areas lie outside of the Inmarsat footprint. The Iridium satellite constellation, on the other hand, consists of 66 interlinked low earth orbiting satellites that move around the earth in polar orbits, thereby offering the best coverage in the polar regions.

The European Maritime Safety Agency has recently awarded a contract for the development and operation of a European LRIT Data Centre as well as associated ASP and CSP responsibility to the French satellite service provider Collecte Localization Satellites offering LRIT service over both the Inmarsat and Iridium systems. The result will be a Data Centre serving in excess of 10,000 LRIT compliant vessels representing twenty-seven EU flag states as well as Iceland and Norway.

Another technology that demonstrates tremendous potential for the implementation of LRIT is the Automatic Identification System or AIS. AIS is an IMO regulated, radio based data communications system with primary applications being maritime safety and vessel traffic management. Like LRIT, AIS collects and transmits a short message packet containing basic information on a vessel. As a minimum, this packet would include a time tagged position report as well as basic information on a vessel and the nature of its voyage. Unlike LRIT, AIS in its current form is limited in range by the radio technology it uses as a medium. Range is normally limited to approximately 20 miles for ship to ship communications and 40 miles for ship to shore communications. Its practical applications are therefore limited to coastal navigation and approaches to ports and harbours.

While there is no mandatory requirement for long range reporting, the AIS performance standard does provide an option for long range applications. In order to overcome the range limitations of the current shore based technology and be adopted as a option to meet long range identification and tracking requirements particularly in the case of open ocean traffic, AIS must evolve to include satellite based communication. As a preliminary step in the acceptance of space based AIS as an approved technology for LRIT, the Norwegian Defense Research Establishment has carried out work to model the performance of a space based AIS receiver deployed on a low earth orbiting satellite for maritime traffic monitoring.

The probability of detecting AIS targets from space and consequently the predicted performance of AIS as a means of meeting LRIT mandatory requirements is dependent on a number of factors. For example, the swath width illuminated by the satellite on the earth's surface, the length of time that a particular point on the surface is in view of the satellite on each overhead pass, and the effect of the density and distribution of vessel targets are all issues that must be resolved before satellite payloads can be specified and space based AIS is adopted as a means to meet LRIT requirements. Regardless, the global implementation of AIS through the deployment of infrastructure by flag states and the installation of shipboard AIS transponders on new and existing vessels continues. When satellite based AIS is ultimately approved as a means of achieving LRIT, the result will enable seamless identification and tracking of vessels from the origin of a voyage through to the destination essentially anywhere on earth.



Mr. Neil Cater is a registered professional engineer with a degree in Electrical Engineering from Memorial University of Newfoundland (1981).

He joined the former Canadian Centre for Marine Communications (CCMC) in July 1999. Following the establishment of the Marine Institute's School of Ocean Technology in 2008, CCMC was repositioned to become the core of the School's Applied Research and Industry Outreach unit. Mr. Cater currently manages a program that provides Applied R&D and industry support in the area of Ocean Instrumentation to marine sector partners as well as to research initiatives within the Fisheries and Marine Institute.

Prior to the creation of the School of Ocean Technology, Mr. Cater served as the director of the SeaComm Program at CCMC. He was responsible for a program that built capacity and competitiveness and seeks global market opportunity for Canada's marine communications industry.

He maintains an active industry presence. He continues to serve as Chair of the Canadian Sub Committee for IEC Technical Committee (TC) 80. This committee provides Canadian interests with a forum and accredited Canadian representatives to IEC Technical Committee 80, which governs international standards for Marine communication and navigation equipment and services. Mr. Cater has recently been instrumental in the formation of the Smart Ocean Sensor Consortium, a group with the common interest in the promotion and adoption of standards for interoperable ocean sensors and serves as the groups first Chairperson.