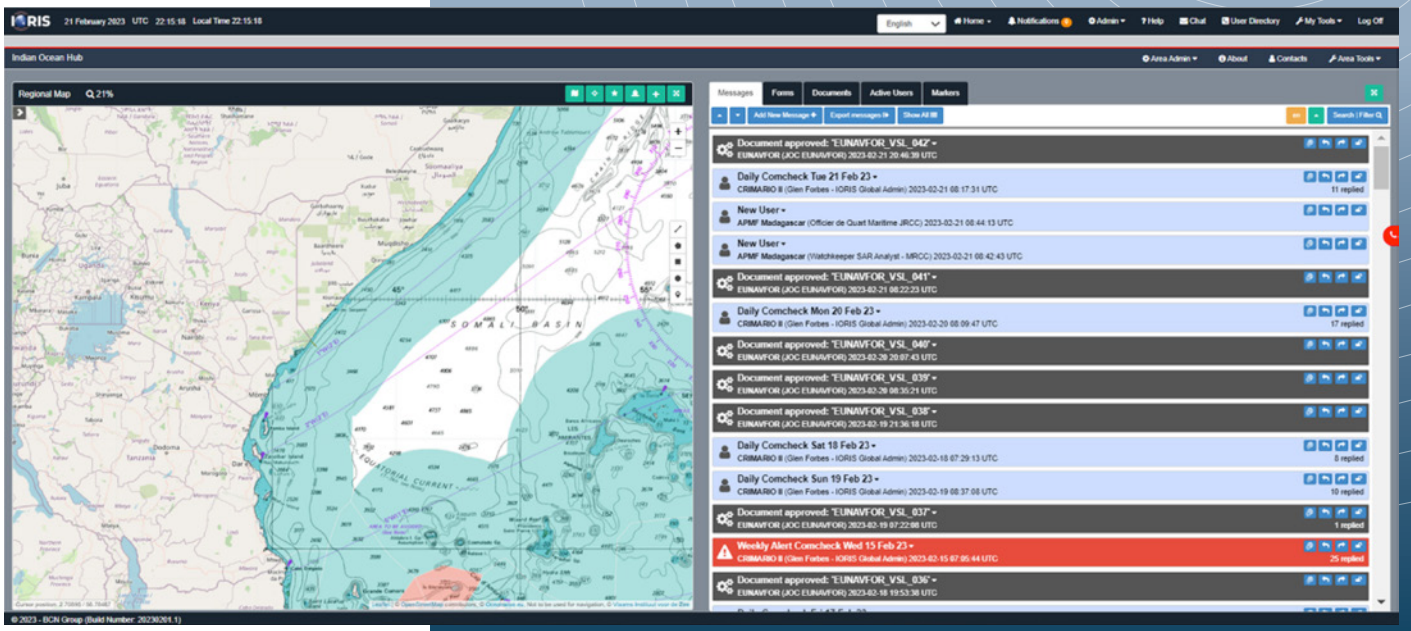
MOVING FROM SITUATIONAL AWARENESS TO SITUATIONAL UNDERSTANDING AND ACTION

CONTENT

THE IORIS SYSTEM

The Indo-Pacific Information Sharing (IORIS) platform developed and launched in 2018, is a neutral, reliable and user-friendly maritime **information sharing tool**, which enables coordination and communications via a secure encrypted online environment. Its primary function, and valuable capability, is to provide maritime centres, organisations and agencies with a means **to analyse, plan and coordinate maritime operations** from the Western Indian Ocean, through Asia and Southeast Asia and across the Pacific Ocean. With the ability to distribute enriched data, including satellite and terrestrial AIS, supported by an integrated Skylight data feed and other bespoke capabilities, IORIS provides users with the unique capability to exchange operational information on a diverse range of maritime threats, in real-time. IORIS connects domestic and international stakeholders to address the evolving challenges manifesting within the maritime domain.

IORIS tailor-made and dedicated community areas (CAs), support the management of day-to-day information sharing, collaboration and monitoring of maritime safety and security operations in support of improving situational awareness and enhancing maritime domain awareness (MDA).



Indian Ocean Hub CA

IORIS is an operational environment, with information related to day-to-day activities of the regional and national entities subscribed to it.

In addition to the operational environment, IORIS also maintains a "mirrored" training environment which provides maritime agencies with the ability to train personnel and conduct operational exercises without compromising the IORIS operational environment.

ACCESS & PERMISSIONS

IORIS is a secure encrypted web-based environment hosted in Microsoft Azure cloud with multi factor authentication. This enables authorised users to access the platform with no special infrastructure required at local level.

CYBERSECURITY MEASURES

IORIS utilises a secure Microsoft Azure cloud hosting environment that ensures data integrity whilst affording secure accessibility to authorised users through an encrypted environment utilising:

DATACENTRE / HOSTING SECURITY

▶ Complies with a vast array of international and country specific information security standards.

▶ Offers Intrusion detection and prevention protocols

▶ Offers Physical site security

AUTHENTICATION AND USER ACCESS CONTROLS

▶ Password Security – offers unique passwords / regular password changes

▶ Two factor authentications – enabled by default for all users accessing the Operational Platform.

ENCRYPTED DATA AND BACKUPS

▶ IORIS data is encrypted using SSL with all pages served on an HTTPS connection while in transit (circulating in the network) and at rest (stored in the servers).

▶ Additional internal 256 AES file encryption is available for sharing sensitive files.

▶ Backup data is encrypted in transit and at rest and performed every 10 minutes and can be recovered up to 35 days.

PENETRATION TESTING

▶ Regular cybersecurity reviews and penetration testing are conducted on IORIS to ensure it meets the ever-evolving global security threats.

A more detailed technical document specific to IORIS security is available on request.

COMMUNITY AREAS AND AREA TYPES

Users are provided with access to their own private 'Home' or 'National' ***Community Areas (CA)***, and/or regional community areas called Hubs, the latter administered by CRIMARIO.

A CA can be used for regional, local or agency communications, the management of activities such as exercises, and the coordination of maritime incidents etc. The CA Administrator invites set of users and only they can participate in the CA activities.

Area Type and Community Area

Coordination between CAs can be achieved by inviting other users on an area-by-area basis, e.g., the Administrator for an incident in one CA can invite users from another CA to participate in the operational aspects of the incident.

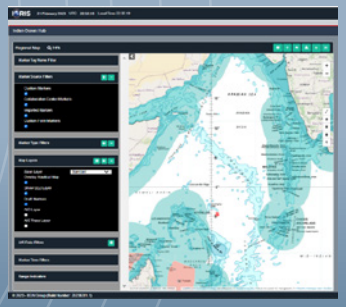
It is important to stress that CRIMARIO staff do not have access to CA's unless invited in by the local Administrator.

The Maritime Directory may be utilised to identify relevant users.

FUNCTIONALITIES

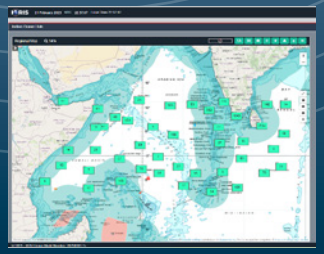
MAPS & LAYERS

The dedicated mapping feature in IORIS displays a scrollable and zoomable view of the entire globe. A user will typically work within a local area of interest, but they are free to move to another area at any time, recognising they only have the ability to see the map, but do not have visibility of the relevant CA's for the area, unless specifically invited. Information on the map is presented in layers that builds an operational view of the Area. Layers include:



Map Layers

- ▶ Base Layer – Represented by Open Street Map Ocean/Land options.
- ▶ EEZ Layers – Two options: EEZ boundary limits / EEZ colour-coded (see image)
- ▶ Nautical Chart Layer – Global layer available showing enhanced charts.
- ▶ Marker Layers – Three types of Markers are selectable layers on the map. These can be searched and filtered allowing the user to focus on a vessel/s of interest (VOI) without unnecessary clutter on the map.



AIS Clustered View

AIS Unclustered View

AUTOMATED IDENTIFICATION SYSTEM

A user can be assigned the permission to view satellite and terrestrial AIS data which is enabled with any given CA. The AIS data is internally updated every 15 minutes displaying vessels based on the user's current area of interest (AOI). Since a large volume of vessel traffic may be displayed, the map uses a 'clustering' process of data points to speed up the display refresh. Greater detail may be selected by zooming in and 'unclustering' to show individual vessels within any given area and vessel information.

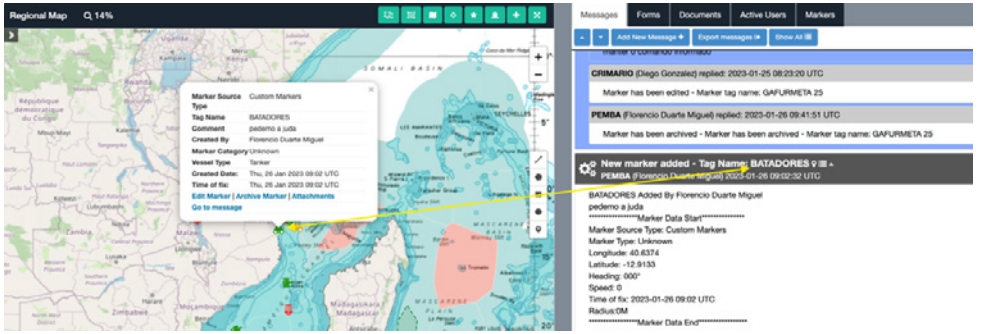
To Note: Maps are not to be used for navigational purposes. Maps in IORIS do not endorse jurisdictional spaces in case of disputes between coastal states.

CHAT MESSAGES & ALERTS

The CA home screen contains a dedicated **Messaging area** that is integrated with the map and supports audible/visual popup Alerts. A User can add a message which will appear immediately on the screen of all users who are using the same CA.

A User message can be configured to generate an Alert (in red), and have a Custom Marker attached (below). The chat integrates with a real-time translation function which can be pre-selected by the operator and will instantly translate messages into any of the languages supported by Microsoft.

Community Area Messaging Area



Messaging, Custom Marker

Both the mapping area, and Messages area can be maximised individually to full screen. This is particularly of benefit in a centre with video wall/large screen/projector capability, especially for incident / crisis management.

PRIVATE CHAT

CA messages are visible to all users in that specific area.

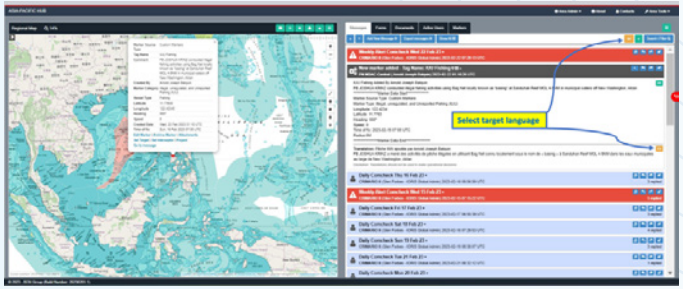
A 'Private Chat function' however, allows conversations between individuals or groups in a separate User Interface (UI). The user creates the Private Chat and assigns the chosen users from the Directory. Users can pick up the chat once online.

The end user will see the unread message count flash in the main IORIS UI, notifying them to join the chat. Any user on the platform may identify other users via the user Directory in the top menu. All messages within Private Chat can only be accessed by the individuals invited. File attachments may also be encrypted for added security between private users.

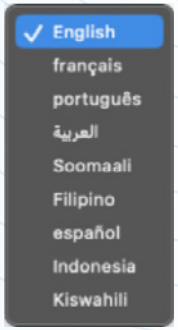
Private Chat

LANGUAGE AND TRANSLATIONS

The main IORIS application menus are designed to work in multiple languages. So far nine languages are available, but more can be added on request. In addition, all chat text can be enabled for automatic language translation and will convert incoming text to any chosen language.



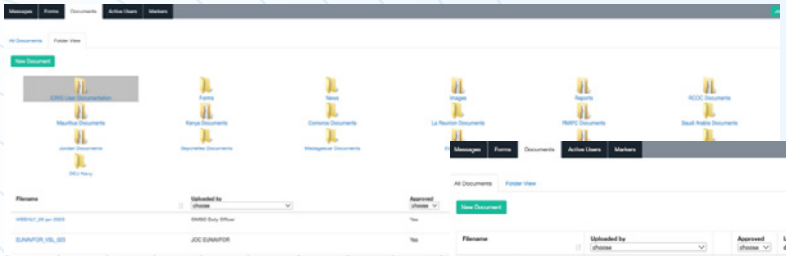
Language Translations



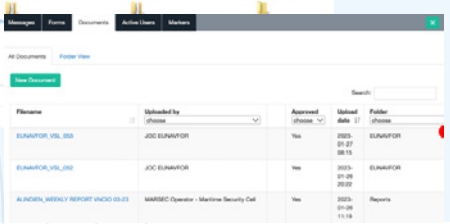
Nine menu languages available

DOCUMENTS

Each CA has its own set of folders for storing uploaded files, including documents, images etc. A Documents Tab allows the user to view shared documents, open, download as required. An additional encryption tool is also available for sensitive files, providing an AES 256 encryption algorithm. The password is assigned by the user and then passed to the recipient by whichever means they choose.



Community Area Folders



Documents Tab

TEMPLATES AND FORMS

The use of 'Forms' can be central to any operational environment and define and distribute information. This built-in template system for defining forms enables users to create their own standard template they can share with other users within their CA or globally. Types of forms could include preliminary alerts and updates for suspicious activity, SAR, IUU, for example. The forms process of drafting and releasing is customisable to meet the requirements of specific centre local SOPs.

IMPORT & EXPORT OF DATA

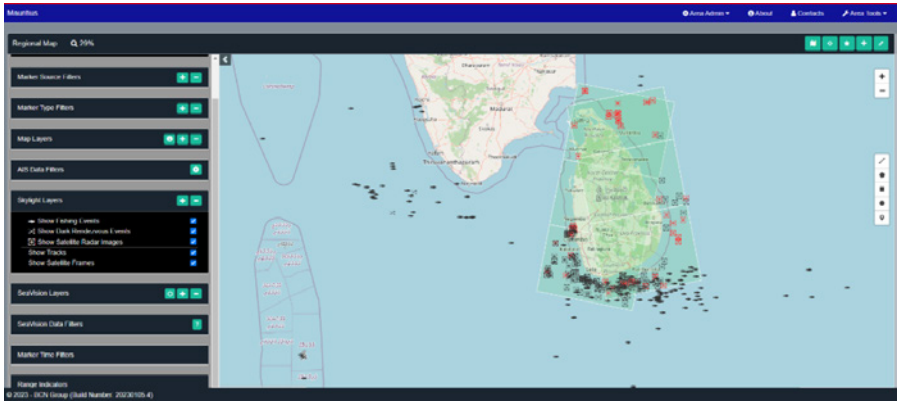
Users can import and export data between CAs where they have the required permissions. For example, messages, forms, markers and documents can be copied and moved to a new CA. This is essential if creating a new area, such as an incident where initial activity around it has already taken place in the parent area. The area administrator may also copy some existing or all the existing users from one area to another, as well as the ability to add new users quickly to participate in the incident, such as Company CSOs or vessel Captains as required.

Data is exported in PDF reports form.

SKYLIGHT VESSEL DETECTION

Skylight data generates events to identify suspicious behaviour that may be illegal or non-compliant with fisheries and other maritime regulations. Events are displayed for vessels around the globe and in user-defined areas. It displays specific interesting events rather than showing all vessels and tracks to reduce the time to analyse tracks. It displays dark rendezvous, satellite radar images and suspicious fishing activities over the preceding 24 hours. The events are categorised as follows:

- Dark Rendezvous events occur when only one vessel transmitting AIS exhibit a track pattern indication a rendezvous with a vessel not transmitting AIS.
- Synthetic Aperture Radar (SAR) data detects vessels that are not carrying AIS or have AIS switched off. It may not necessarily be illegal or suspicious, but is useful to identify vessels: in Dark Rendezvous'; entering marine protected areas or EEZs without authorisation; and/or conducting abnormal or suspicious activities.
- A Fishing Event is generated when fishing behaviour is detected in the tracks of an AIS-transmitting vessel. Machine learning detects four types of fishing: trawling, longlining, purse seining, and squid jigging.



Skylight Events Layers On

TRAINING

The Training platform offers simulated operational environments for use in the training of information sharing and in familiarisation with the operation and management of IORIS. The Training platform mirrors the Operational platform in all respects even using the same data feeds for mapping etc. Training has been conducted in East Africa, Asia, Southeast Asia and across into the Pacific.

IORIS Training to [illegible]

ANNEX A

IORIS IN SUPPORT OF INFORMATION EXCHANGE AMONG NAVAL FORCES AND THE MARITIME INDUSTRY

The dramatic surge in piracy in the Horn of Africa, led to a situation in which several navies were, and still are, operating in common areas, with common goals, but under different chains of command. Existing information sharing tools used in the Indian Ocean, usually only allow access to official bodies such as navies, law enforcement agencies, Maritime Rescue Coordination Centres (MRCC), etc, but not the merchant navy community.

In this context, IORIS offers a platform that facilitates the free flow of information and data amongst navies, at the operational and tactical level, including with relevant civilian agencies. IORIS provides users with the capability to de-conflict operational activities, coordinate operations and offer data relating to incidents, such as alerts and images, private chat. This level of collaboration is key for the safety and security of seafarers transiting across precarious oceanways.

But the dramatic surge in piracy in the Horn of Africa led to a close partnership being developed between the shipping community and naval forces. This implied a need for naval forces to better understand maritime industry's concerns and interests. Crucial to this relationship is the building of trust, through the provision of enhanced information sharing. This partnership reinforced the concept of Naval Cooperation and Guidance for Shipping (NCAGS).[1]

IORIS provides the foundation for near real-time information sharing and enhanced collaboration. Information shared via IORIS can be as diverse as:

- industry Releasable Threat Assessments and Bulletins;
- data pertaining to statistics such as the use of privately contracted armed security personnel (PCASP) and ship protection measures (SPM);

IORIS allows vessels registering on any voluntary registration/reporting scheme online, to: report maritime incidents or events, receive updates on incidents, receive information on threat areas, recommended transit corridors and sailing recommendations, etc.

It could also allow merchant vessels to communicate discreetly with one another when navigating within a common CA, apart from also communicating with coastal safety and security centres, given the option to select a low bandwidth.

Merchant vessels which decide to join CAs administered by naval forces, tied to Voluntary Registration / Reporting scheme, would be assured that commercial sensitive data will be protected.

(1) NCAGS promotes cooperation between military and civil maritime authorities and agencies, and merchant shipping - NATO publication ATP-02,1 Guide to Owners, Operators, Masters and Officers. Available at https://shipping.nato.int/systems/file_download.ashx?pg=1791&ver=50

ANNEX B

IORIS IN SUPPORT OF PROTECTING SHIPPING AGAINST EXTERNAL AGGRESSORS (PIRATES, ARMED ROBBERS, TERRORISTS[2])

Merchant ships transports over 80% percent of global trade,[3] relying on secure trade routes, especially chokepoints which, at certain points, could pose a risk to shipping. These chokepoints are identified as being at higher risk to the safe and secure passage of vessel and crew. The Bab el-Mandeb Strait and Strait of Malacca being identified as piracy prone areas, whilst the remainder, such as the Suez Canal, the Strait of Hormuz and the Panama Canal may be considered vulnerable, and could affect commercial/security concerns.

In this respect, IORIS may be used by regional maritime reporting centres to monitor vessel movement, enabling reporting points, the exchange of security and safety-specific information and data, to address piracy, armed robbery and maritime terrorism.

Importantly, in conjunction with internationally recognised global security and safety systems, such as GMDSS, VHF Channel 16 and Ship Security Alert System (SSAS), the IORIS system enables MRCCs to receive and discreetly transmit piracy-based alert messages relating to any incident encountered. Additionally, notifications of safety concerns may be exchanged within any specific MRCC CAs, similar to the Notice to Air Missions (NOTAMS) notifications.

Moreover, the ability to exchange information across regional boundaries, reporting zones, high risk areas (HRAs), Joint War Committee Listed Areas or any designated Voluntary Reporting Scheme is a key component of the provision of the IORIS system.

IORIS enables collaboration amongst MRCCs, maritime Operations Centres, naval units and likely law enforcement agencies, in support of the merchant shipping community, streamlining processes and providing a means to mitigate risk in any given piracy-related/armed robbery/terrorist situation.

(2) CRIMARIO is not endorsing of providing any specific criteria to classify a given event as a terrorism.
(3) Source: https://unctad.org/meeting/launch-review-maritime-transport-2022. Access February 2023.

ANNEX C

IORIS IN SUPPORT OF COUNTERING ILLICIT TRAFFICKING

Combating illicit trafficking by sea requires the employment of sound tactical skills coupled to a profound knowledge of applicable laws and regulations, combined with flawless inter-governmental and regional coordination. Whilst the former two ingredients much depend on the State to prepare its human resources to address maritime threats, IORIS can support law enforcement operations given its unique functionalities including:

• the chat (group/private) function, the document sharing function and the forms function, which facilitate enhanced maritime domain awareness and the exchange of information between national and regional administrations.

• detailed charts and associated tools, including: AIS; Skylight - to identify dark rendezvous detection at sea; and interception calculations;

• the ability to create tailor-made Community Areas allowing operators to define which authorities / regional partners will join the operation;

• the flexibility to add new users to join Community Areas on the spot, with varying access rights, allowing for swift information-sharing and prompt decision-making, adapting confidentiality limitations as required. This allows operators, as well as judicial, administrative or political authorities, to determine the level of involvement of other players.

• the provision of communications and coordination node to link regional operations centres together. Recognising that IORIS is a web-based portal, it allows users to have the ability to follow operations, and respond to queries, from personal devices outside normal office hours;

• if adequate bandwidth is available, vessels at sea can log into Community Areas established by maritime operations centres (MOCs), to facilitate the conduct live operations. MOCs are able to upload information into the interactive map such as sightings of suspect vessels identified through radar, radio frequency detection or aircraft sighting. In the event of reduced bandwidth, vessels at sea have the ability to maintain the information and messaging exchange protocols, while disabling the IORIS mapping functionality.

• Messaging which cannot be deleted or modified, and can be download as a PDF document, supporting the submission of evidence.

ANNEX D

IORIS IN SUPPORT OF SUSTAINABLE FISHERIES

Enforcing fisheries laws and regulations on the outer perimeter of Exclusive Economic Zones, and on the High Seas, is invariably difficult because fishing vessels are all too often beyond the grasp of law enforcement assets. Additionally, if monitored electronically via Vessel Monitoring Systems (VMS) or AIS, the vessels have the option to go dark. Moreover, the practice of exchanging processed information between flag, port, coastal States and regional organisations, is hampered given a lack of tailor-made information-exchange tools amongst stakeholders. IORIS offers a myriad of solutions to States and fisheries organisations, to enhance monitoring, control, surveillance and enforcement operations, through the platform's three main functionalities as follows:

Internal / External Communication

IORIS offers real-time and encrypted communications for agency, interagency and regional exchanges (Port State Measures Agreement (PSMA) Article 6), to:

• Send/receive notification and alerts concerning suspicious IUU fishing activities;

• Share information about fishing vessels; and

• Transmit inspection results to the flag State (PSMA Article 15).

IORIS is able to offer this through:

• Private/group chat, with translation functionalities, eliminating language barriers.

- text messages sent through IORIS cannot be amended or changed
- text messages can be downloaded in PDF, for evidence in court.

• Voice over IP

Regional and Interagency Coordination (PSMA Article 5)

IORIS is the optimum interagency tool allowing seamless coordination of operations amongst fisheries, port, customs, health and coast guard authorities, to:

• Coordinate High Seas and EEZ surveillance operations.

• Coordinate interagency inspections prior to the arrival of fishing vessels in port (PSMA Article 8) and inform all agencies concerned of port denial;

• Integrate fisheries related port State measures with port State controls;

IORIS offers excellent coordination functionalities such as its ability to:

• Plot and share fishing vessels' positions/ marine protected areas on maps;

• Import data from other systems including satellite data and VMS;

• Create standard templates e.g. Advanced Request for Port Entry (PSMA Annex A);

• Share and archive documents/files containing F/V licences, IUU history, etc

Surveillance Functionalities

IORIS offers a limited amount of surveillance data including:

• Automatic Identification System (Satelite AIS);

• Skylight Artificial Intelligence – automatic detection of possible dark targets

• Potentially in the future, on an ad hoc, basis for coordination of operations:

- Copernicus satellite data
- Detection of radio frequency emissions at sea

ANNEX E
IORIS FOR VESSEL TRAFFIC MONITORING

The scope of vessel traffic monitoring is to anticipate precarious situations, by implementing interrogative procedures, reporting obligations, and passive surveillance of maritime approaches. This implies that merchant shipping would be linked with maritime safety centres and port controls through IORIS since the latter shipping need to forward documentation efficiently in any passage or stopover.

Government to Government

If a country has access to AI-type analysis of shipping movements, with automatic alerts, the following maneuvers can be detected for close observation and action as necessary.

• Vessels navigating close to shore, erratically, and/ or at slow speed;

• Vessels on course for a grounding;

• Vessels navigating outside/blocking traffic separation schemes;

• Vessels not under command or restricted in their ability to manoeuvre; and

• Vessels on collision courses

IORIS could offer a channel of communications amongst Vessel Traffic Monitoring (VTM) Centres, to warn each other about inconsistent vessel maneuveres divulged above.

Shipping to Maritime Safety Centre / Port Control

Ship-to-Shore: In accordance with the provisions of the MARPOL Convention, ships must report information relating to defects, damage, deficiencies, or other limitations as well as, if necessary, information relating to pollution incidents or loss of cargo. Whether for ports, entering territorial waters or EEZs, and depending on their type of cargo, these ships must regularly report the same information to the different ports and countries they pass through, the reports including:

• MOUVINF movement information

• SHIPREP, ship report in case of deficiency

• SURNAV, if the vessel is transporting IMO class type hazardous materials.

IORIS offers opportunity to standardize the sharing of reports on a regional basis, and ships in transit would no longer have to declare themselves each time they pass through neighbouring Exclusive Economic Zones, forms being available in the IORIS database and shareable with the various MRCCs, VTMs or ports would be issued.

Coastal Station Reports: Shipping companies, ports, MRCCs, VTMs, local agents and vessels underway can receive local navigational warnings if inside a national CA.[4]

(4) No statement included in this brochure should be interpreted as reflecting any intention to replace or alter established GMDSS MASTER PLAN, SAR PLAN or defined SRR or any disposition included in the relevant Treaties and Conventions.

ANNEX F
IORIS IN SUPPORT OF SEARCH AND RESCUE COORDINATION

Global search and rescue (SAR) and Global Maritime Distress and Safety System (GMDSS) Master plans are implemented by IMO signatory members and readily available through IMO approved channels.[5]

The prompt response to distress incidents at sea are of paramount importance to preserve the safety of seafarers, communications through GMDSS playing an essential role, as is the coordination of rescue operations thereafter by Joint Rescue Coordination Centres (JRCC) and MRCCs.

IORIS can support the coordination of rescue operations in two areas:

• if GMDSS connectivity is low in remote coastal regions, and a satellite link is available to the ship, IORIS can reinforce communication means for vessels to receive and send SAR related data, and support in the conduct of SAR operations;

• Merchant vessels logging into IORIS could plug into Community Areas (virtual chat groups) to support search and rescue coordination centres in the conduct of operations, given the graphic display of search patterns, the position of rescue assets, etc.

On the government-to-government level, IORIS link can link JRCCs / MRCCs, which enhance the coordination of SAR incidents at sea, and can relay important request such as asset sharing, etc.

Should a coastal State so desire, it could create a national IORIS search and rescue region (SRR) CA, into which merchant vessels can opt to plug into on a voluntary and routine (non-distress) basis. This way the JRCC / MRCC can provide updates on navigational safety and security warnings through satellite link, with the added value of offering a virtual communications platform (private/group chat) with a simultaneous text translation; sharing of documents; and the possibility to post alerts and information on any incident in progress.

(5) No statement included in this brochure should be interpreted as reflecting any intention to replace or alter established GMDSS MASTER PLAN, SAR PLAN or defined SRR or any disposition included in the relevant Treaties and Conventions.

ANNEX G

IORIS IN SUPPORT OF COMBATTING MARINE POLLUTION

Between 2000 and 2021, maritime freight volumes nearly doubled, leading to an aging global fleet and a shift of older ships towards the southern hemisphere. This trend has increased the risk of pollution by ships discharging bilges / dumping waste under lax regulation and accidents caused by poor maintenance.

To address these issues, states are investing in more advanced detection and response capabilities to protect the environment and fisheries resources. Cooperation between states is crucial, particularly given the fact that intentional acts of pollution often occur in international waters.

IORIS enhances anti-pollution capabilities by improving information sharing and coordination among states, increasing detection capabilities, and facilitating more effective responses to pollution incidents.

This is because the IORIS platform facilitates communication and coordination among states, to monitor and share information on ships discharging bilges and other waste into oceans, to dealing with major calamities at sea, where the pooling of resources is essential to address major calamities.

More specifically, IORIS:

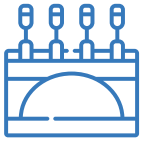
- allows authorities to assess past vessel movements through limited AIS historical data to determine those potentially conducting bilging operations;
- facilitates the plotting of pollution markers on its common operational picture;
- allows for the reporting of pollutant location and drift; and
- facilitates coordination cleanup operations between states, command centers, and on-scene cleanup assets.

In the coming months, CRIMARIO intends introducing functionalities into IORIS which would support States monitor pollution situations through the provision of satellite data.

If looking at past cases, IORIS could have been of value to coordinate operations dealing with the MV X-Press Pearl, which sunk off the coast of Colombo with 1,486 containers on board. This, not only disrupted vital shipping lanes, but seriously impacted the marine environment due to the chemicals and plastic nurdles that were carried in her containers.

ANNEX H

IORIS IN SUPPORT OF PROTECTING CRITICAL INFRASTRUCTURES



Critical maritime infrastructures are essential for a country's sovereignty because it enables the government to exercise control over its territory and ensure the well-being of its citizens. Without critical infrastructure, a country would be unable to provide essential services to its population, defend its borders, or maintain economic stability.[6] Examples of such infrastructures include power stations, offshore oil platforms, reverse osmosis plants and the undersea cable network. These need to be protected, to prevent, and address, calamities caused by intended human action or error, or the impact of severe weather.

Terrorist organizations have the capacity to take advantage of the vulnerable maritime domain, to target ships, harbour infrastructure, and permanent platforms at sea in order to inflict devastations like the recent tragedies. The weapon of choice is undoubtedly the improvised explosive device, which may be used with offensive strategies to target specific infrastructure in the marine and cyber domains. Another evolving hazard of significant nature is the widespread proliferation of autonomous vehicles.

Human errors can also lead to disastrous consequences such as when the massive container ship Ever Given blocked the Suez Canal for six days. Ever Given's distress completely stopped all ship traffic through the Suez Canal, causing a crisis that cost the world economy almost 2.5 billion euros. It demonstrated the terrible results of blocking a choke point. Another noteworthy example of the devastating consequences of human error is the major explosion in the port of Beirut which caused at least 218 deaths, 7,000 injuries, and US$15 billion in property damage, as well as leaving an estimated 300,000 people homeless.

It is only the relentless efforts of the coastal states and organizations, acting both individually and collaboratively that such calamities can be prevented, and addressed if tool late. But these incidents demand intense interagency operations, dependent on secure and user-friendly software tools to facilitate full collaboration.

IORIS is the optimum interagency tool to support the coordination of security and safety operations, to address potential threats and hazards from the littoral environment, and coordinate crisis management measures if ever an incident occurs.

(6) Artur Lucas da Silva, A short reflection on [Maritime] Critical Infrastructures protection, LinkedIn, 30 March 2023.

ANNEX I
IORIS IN SUPPORT OF HARBOUR MASTER AND PORT OPERATIONS

Maritime transport is the backbone of international trade and the global economy with over 80% of goods in international trade carried by sea, and the percentage is even higher for most developing countries.[7] These figures reveal how important ports are for trade, and ultimately for the welfare of people all over the World. IORIS can support complex port operations and security/safety infrastructures and procedures.

Whilst IORIS is as yet not being used for harbour masters and port operators, this is currently being explored with international shipping associations and shipping companies.

Port call requests / Anchorage/Mooring: Vessels can request permission to make a port call, through anchorage/mooring requests via a dedicated form for each port on IORIS.

Vessel Pre-arrival messages: Vessels approaching port could send pre-arrival messages (whether directly or through Shipping Agents) offering a Single Window for multi-agency for the following information:

- Crew list
- Passenger list
- Cargo manifest
- Maritime declaration of Health
- Declaration of Hazard cargo on board
- Waste and residues,
- Change of shipping agent,
- Visualization of Ship's Clearance

Port Information: Berthing place allocation, ISPS Information (including security level in place), information on works in progress, MARPOL facilities and regulations, inspections, anchorage areas, monitoring of secured anchorages, local navigation warnings are all examples of typical port communications which IORIS can disseminate as single window for vessels calling at any given port, including online forms, and communications in real time with the additional value of translation functionalities.

(7) Source: https://unctad.org/meeting/launch-review-maritime-transport-2022. Access February 2023.

ANNEX J
IORIS IN SUPPORT OF PORT SECURITY

Ports are the link between seas and land, playing a pivotal role in trade and shipping of goods, essential to economies and the welfare of nations. The adherence to relevant treaties and conventions and the implementation of security levels and security plans, therefore, have a positive commercial impact.

Port facilities serving ships engaged on international voyages fall within the scope of the International Ship and Port Facility (ISPS) Code.[8] This code offers a comprehensive approach to protecting an identified list of assets, essential for the interaction (interface) between port-ship, ship-ship, ship-terminal, etc. The conduct of risk assessments leads to the development of port facility protection plans and port security plan as a whole.

IORIS is a secure platform that can support port security, offering a collaborative tool for port facility security officers, port security officers, ship security officers and pertinent port authority officials, offering a secure medium through which operations can be coordinated and compulsory documents, statements, plans, etc. exchanged, most notably:

- the security level established by national authority;
- additional security measures implemented;
- list of assets to protect;
- port plans;
- access control points;
- surveillance systems;
- risk assessments approved by pertinent authority;
- Port Facility Protection Plan;
- General Port Security Plan;
- Contingency plans;
- Critical Infrastructure Protection Plans.
- Declarations of Security.

A tool to calculate risk assessments by port authorities, or pertinent element according to national regulations, can be integrated into IORIS, which will serve as the foundation for the development of a Port Facility Protection Plan, including protection measures that could ultimately suppress or mitigate potential risks.

Finally, IORIS provides AIS which is an added value for port authorities monitoring shipping movements inside harbour.

(8) No statement included in this Brochure/Annex should be interpreted as reflecting any intention to replace or alter established provisions in SOLAS Convention, in particular Chapter XI.2, or ISPS Code, or any disposition included in the relevant Treaties and Conventions.

CONTACT US

For further information on the CRIMARIO II project:
martin.cauchi-inglott@crimario.eu

For IORIS system administrative matters:
ioris.admin@crimario.eu

For IORIS system training advice:
bjorn.beirens@crimario.eu

www.crimario.eu

FOLLOW US :

IORIS is a CRIMARIO initiative

CRIMARIO II
INTERCONNECTING THE INDO-PACIFIC

Funded by

Implemented by EXPERTISE FRANCE
GROUPE AFD