Full-spectrum Maritime Domain Awareness

Establishing and Maintaining Complete Security over Coastal Waters

Abstract

With so many disparate sources of situational intelligence available from coastal waters, maritime security operators are often overwhelmed by a tsunami of critical information. To manage this massive amount of intelligence information and establish true maritime domain awareness, maritime agencies need a system that will streamline the flow of intelligence from all sources. The system must be designed to process information quickly and efficiently to enable effective analysis and decision making by multiple maritime security agencies. The CoCommand solution provides operators contextual visualization of a maritime area based on human-centered design principles. It is built on complete sensor and information fusion on a single master domain data management framework. This single, integrated framework provides a complete and accurate, near real-time picture of any maritime situation based on synthesized data from all sources — satellite, terrestrial, radar, reference, contextual, and predictive. It also enables multi-layered analysis of a variety of intelligence data, including signals, imagery and human intelligence.

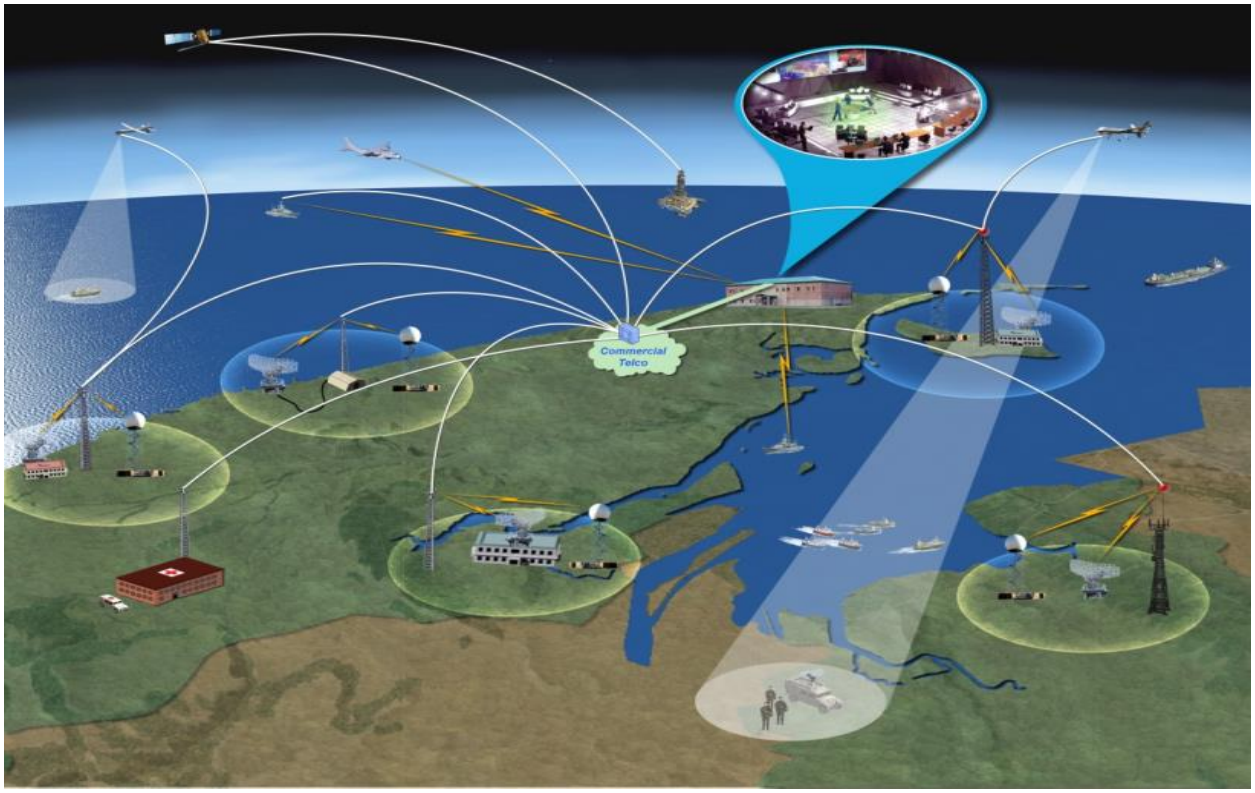
Table of Contents

List of Illustrations

The Maritime Security Challenge

Fishing, trade and oil exploration are major contributors to the economic health of countries with extensive coastlines. For this reason, port, vessel, and facility security are key concerns in coastal waters. Establishing and maintaining that security requires ongoing monitoring of the activities of commercial freighters, fishing boats, pleasure craft, ferries, water taxis, oil and gas exploration vessels, energy platforms, military vessels and coast guard ships (Figure 1). At the same time, clandestine activities, such as smuggling, illegal and unregulated fishing, dumping, and even piracy, must be identified.

Figure 1: Multiple vessels in coastal waters complicate maritime security efforts.



But with so many vessels in the water, protecting maritime assets and maintaining complete security over coastal waters is a difficult task. Every vessel and platform has multiple data attributes that must be continuously tracked. This information must be cross-referenced with the data from multiple maritime sensors, which may include:

- **Acoustic intelligence (ACINT)** from a variety of sources, including hydrophones, geophones, SONAR and artillery ranging systems
- **Human intelligence (HUMINT)** from information collected and provided by in-field personnel, intelligence and counter-intelligence agents, and special forces, as well as allies

- **Imagery intelligence (IMINT)** from photographic, radar, electro-optical, infra-red thermal and multi-spectral sensors, which can be ground-based, seaborne, or carried on overhead platforms
- **Measurement and signature intelligence (MASINT)** from quantitative and qualitative analysis of metric, spatial, wavelength, time dependence, modulation, plasma and hydro magnetic information collected from technical sensors
- **Open source intelligence (OSINT)** from public sources of information, such as radio, television, newspapers, magazines, journals, technical papers, books, manuals, and the Internet
- **Radar intelligence (RADINT)** from radar detection systems
- **Signal intelligence (SIGINT)** from the interception of communications and communications systems, and from technical assessment of electro-magnetic non-communications emissions caused by radar and missile guidance systems

Unfortunately, with so many disparate sources of situational intelligence, maritime security operators are often overwhelmed by a tsunami of critical information. Although all this information is needed to enable operators to establish complete situational awareness, managing, correlating, analyzing, synthesizing, and processing the information into a concise and coherent maritime overview is challenging.

To eliminate the information tsunami and enable operators to establish true maritime domain awareness, maritime agencies need a system that will streamline the flow of intelligence data from all sources of information. The system must be designed to process information quickly and efficiently to enable effective analysis and decision making by multiple maritime security agencies. Therefore, the system must be engineered to filter, collate, organize, format and present a variety of reliable and relevant intelligence in a manner that supports efficient evaluation and analysis. It must present the combined knowledge of all sensors and intelligence sources available. It must provide access to the ownership and management chain surrounding any vessel in the water, which may extend through many countries because ships spend their economic life moving between different jurisdictions, often far from their country of registry. Plus, it must deliver available intelligence in real time. Only then can operators use the information at their fingertips to develop accurate situational awareness.

With accurate situational awareness, commanders and decision makers can weigh operational options, make assumptions, and estimate results. They can develop specific courses of action, if required, and initiate strategies that will ensure security objectives, including maritime, are met. And they can make final decisions that can be easily communicated to all agencies: maritime, military, security, environment, immigration, etc….

Creating and Maintaining Maritime Domain Awareness

An effective and efficient system that enables maritime agencies to establish and maintain complete security over coastal waters must support wide area vessel surveillance, provide access to intelligence from all sensors and available information databases, and integrate and display all this information in an easy to understand format. The data processing and display system must be backed by decision support software, which can continuously monitor all vessel activity and automatically alert operators to violations, risks or security intrusions in both real-time and predictive modes. This capability should be supported by an integrated and comprehensive geographic display that can immediately provide operators with detailed information on any vessel in the water. With these capabilities, the system will significantly improve maritime surveillance operations and decision making while reducing operator workload and fatigue.

But creating an integrated system that is capable of delivering this functionality presents a number of challenges.

Data Flow

Because information is being collected from a variety of sources and delivered by disparate systems using a variety of protocols, the flow of intelligence data must be continuous and unimpeded. Therefore, the system must easily interface and interoperate with all the sources feeding it and enhance the flow of critical data by supporting an open exchange of data. In addition, the system must be able to manage all the different protocols being used to ensure semantic interoperability in the processing of information based on different definitions of key words.

Information Delivery

In addition to delivering the data, the system must be capable of processing multiple inputs in real time and delivering all the information in an easily digestible and understandable manner. It must process relevant information and present both superior and inferior layers of intelligence in a format that allows operators, commanders and decision makers to review and manipulate all the elements of a Common Operating Picture (COP) as required. This includes information from a Recognized Air Picture (RAP), Recognized Land Picture (RLP), Recognized Maritime Picture (RMP), Recognized Operational Support Picture (ROSP) and Recognized Cyber Picture (RCP). Plus, the system must be able to process supporting information, such as threat assessments, to provide maritime security agencies with a complete, integrated view of all relevant intelligence.

Collaboration

To ensure all information delivered enables effective decision making, the system must also facilitate efficient, real-time collaboration at all operational levels, with all personnel and external agencies. This requires application and information exchange models that are compatible with legacy systems, as well as emerging systems. It requires a system capable of generating a shared COP that supports concurrent workflows over distributed platforms. And it requires support for a variety of integrated processes, including operations planning, operations control, incident management, intel functions, support functions, and information management.

Security

Beyond delivering intelligence information, the system must also be engineered to achieve all objectives while maintaining the highest level of security. To support this type of operational requirement, enable efficient and dependable data flow, information delivery, and collaboration in a dynamic command and control environment, the security system must use integration strategies that converge legacy single-level applications into a multi-level framework. And it must use existing certified and accredited information assurance technology. In this way, the system can ensure that security requirements are addressed in a trusted and secure manner at all levels and in a way that does not disrupt or impede operations.

Simplifying Complexity with Human-centered Design

Finally, because how operators interact with information is more important than the quantity of information available, it is imperative that the technology be intuitive and easy to use. Establishing and maintaining full-spectrum maritime domain awareness can be difficult to achieve if the systems and interfaces delivering the information are difficult to use and understand. Therefore, the system must be built on human-centered design (HCD) principles, which optimize systems and their user interfaces based on how people can, want, or need to work (Figure 2).

Figure 2: An effective maritime surveillance system must be built on human-centered design principles.

The General Dynamics Maritime Surveillance and Security Solution

General Dynamics enables full-spectrum maritime domain awareness with an integrated, full-featured system built around the CoCommand decision support tool for use in operations and command centers.

CoCommand is engineered to integrate a wide variety of situational awareness data and turn it into actionable knowledge. It allows maritime security agencies to weigh options, make assumptions, and estimate results based on specific courses of action and plans that will ensure security objectives are met. These plans can then be easily communicated to sister agencies and executed at the operational level. Once orders are issued, CoCommand allows a two-way flow of information so that all command centers can monitor results and adjust tactics to changing in-field conditions.

Complete Information Fusion

The CoCommand solution provides operators contextual visualization of a maritime area based on human-centered design principles. The visualization is built on complete sensor and information fusion on a single master domain data management framework. This single, integrated framework provides a complete and accurate, near real-time picture of any maritime situation based on synthesized data from all sources — satellite, terrestrial, radar, reference, contextual and predictive. And it enables multi-layered analysis of a variety of intelligence data, including signals, imagery and human intelligence.

The complete, integrated CoCommand solution makes it easier for operators to receive, correlate, analyze and disseminate information in real time. This is enabled by advanced surveillance and analysis features, which include:

- **Situational awareness**, which enables the system to collect and correlate Automatic Identification System (AIS), Long Range Identification and Tracking (LRIT), and imagery data to produce a near real-time geospatial picture of a maritime domain
- **Multiple data-source correlation**, which reads, processes and correlates spatial, geospatial, structured and unstructured data from multiple data sources to generate a multi-faceted view of critical elements in the maritime domain
- **Forensic search and rule generation**, which uses multiple maritime criteria, including ship details, cargo, crew, owners, inspections, history, and positions, and saves the searches as system rules that generate alerts when proximity or geographic electronic fences have been tripped
- **Automated threat evaluation**, which conducts automated threat evaluation as data is received and provides a dashboard with high-threat ships to enable deterministic threat modeling
- **Detection/notification fidelity**, which detects changes in dynamic data from all database sources and immediately runs the changed or added data through a threat evaluation mechanism. ,These detections include a change in threat level for a ship or arrival, a change in dynamic data, proximity violations, and geographical electronic fence violations
- **Alert notification web service**, which uses a variety of web-based information services to notify machine clients about new/changed arrivals and threat level changes

- **Historical data and results tracking**, which maintains a history of the results of the threat evaluation mechanism based on changes in threat level over time for individual ships and arrivals
- **Sense-making mechanism**, which incorporates a sense-making capability that evaluates dynamic use cases and historical data

Utilities

These advanced features are leveraged to provide operators with powerful utilities designed to simplify the maritime surveillance process.

To enable efficient and effective information analysis, CoCommand includes three key utilities that allow operators to define an area of interest and identify potential threats within that area:

- **Geographic fence analysis**, which allows operators to define geographic areas of interest for monitoring of surface targets. Alerts and rule violations can be generated upon the violation of these areas of interest by intruding surface targets. The surface targets can be defined by a multitude of data attributes related to the vessels and their voyages as specified by an operator via the advanced forensic search capability
- **Proximity analysis**, which allows operators to define proximity-based rules and alerts using the geospatial information that is supplied to the system. Proximity analysis is based upon the distance and rate of closure of that distance between two selected surface targets, which can be defined using the advanced forensic search capabilities for a multitude of data attributes
- **Motion analysis**, which allows operators to define heading- and speed-based alerts and rules with the geospatial information that is supplied to the system. These alerts or rules can be tied to specific sets of vessels by using the advanced forensic search capabilities

Once an area of interest has been established and the rules within that area have been defined, operators can configure CoCommand to provide more specific information about any vessel of interest with:

- **Configurable threat views and scenarios**, which allow the system to be configured to create views of a threat matrix associated with a vessel and its voyage in coastal waters. The threat level is calculated based on pre-defined parameters and operators are able to create custom threat views based on all rules, as well as custom views, such as a “safety view”, or “security view”, or “terrorism view”. Each view can have its own threat level ranges and threat level calculation thresholds
- **Suspicious vessel tracking**, which allows the system to track vessels that do not have International Maritime Organization (IMO) numbers. This is achieved through the correlation of vessel data from multiple sources and cross-referencing with other data, such as flag and call sign
- **Threat delta notification web service**, which enables the system to detect a change in the threat level of a vessel or its arrival information and notify interested external applications based on a threat evaluation rules engine

To ensure operators have complete control over all information available at all times, CoCommand also includes utilities that allow the operator to easily access a variety of information sensors and systems:

- **Alerts manager**, which provides operators with access to a dashboard that consolidates the various violations relative to stored criteria for:
    - A geographical electronic fence
    - Distance between two targets
    - Movement analysis of a surface target
- **Status manager**, which provides operators with access to a dashboard that consolidates the surface target count based on:
    - Type of vessels (tanker, bulk carrier, etc.)
    - Flag state of vessels
    - Evaluated threat perspective of vessels (guarded, high, low, etc.)
- **Layer manager**, which provides operators with access to a dashboard that consolidates the various active layers on the viewed interface, including:
    - AIS surface targets
    - AIS threat tiles for a Sea Line of Communications (SLOC)
    - AIS surface target trails
    - LRIT surface targets
    - LRIT threat tiles for a SLOC
    - LRIT surface target trails
    - Data display layers
    - Areas of interest
    - Incident layers
    - Geographic fences
    - Numerous other data inputs from radar, satellite, sensor etc.
- **Go to location**, which provides operators with access to a dashboard where they can input any geospatial location and the system will reconfigure the view to that particular area and present all surface targets in that area.

Finally, CoCommand also includes two utilities designed to extend the reach of an operator’s sensors and systems, when needed:

- **Selector for vessel of interest**, which provides operators with access to a dashboard where they can add and follow vessels of interest globally
- **Selector for arrival of interest**, which provides operators with access to a dashboard where they can configure a particular seaport in the world and monitor vessels arriving in that port

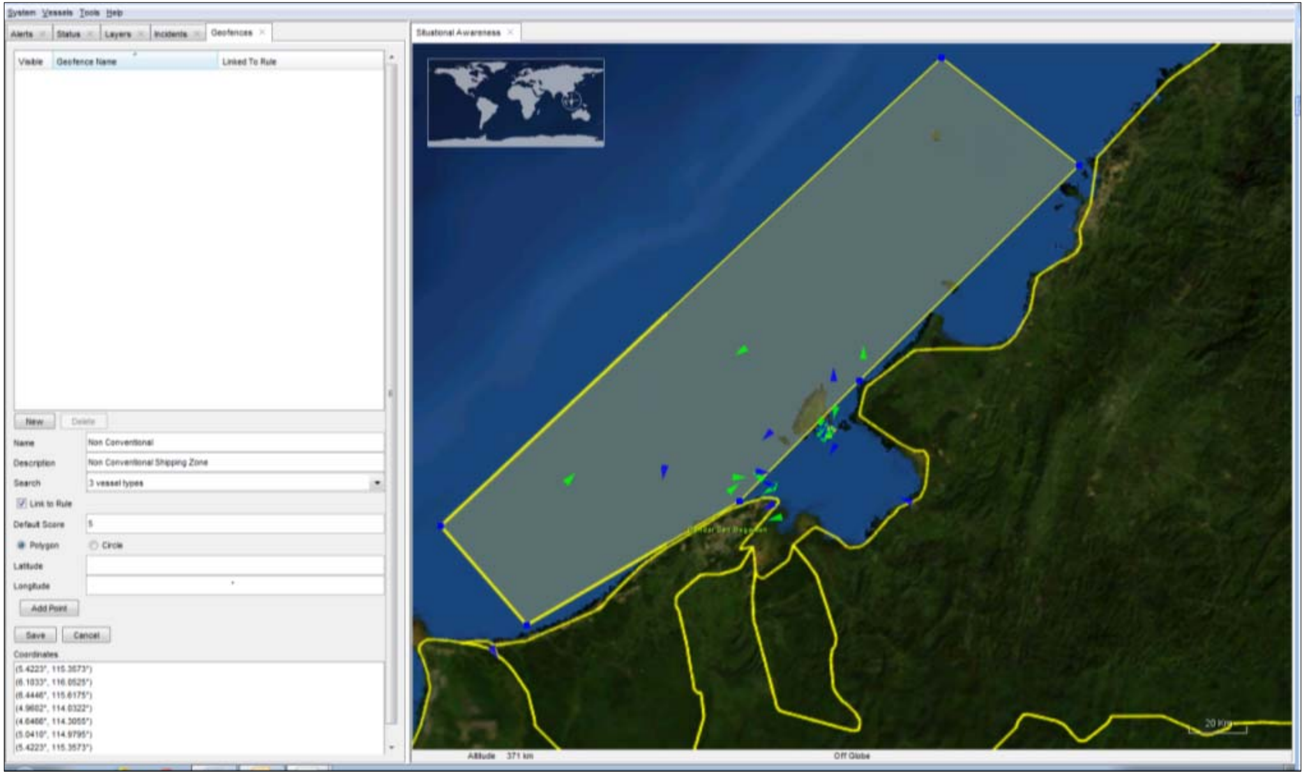
Applying the Solution

The General Dynamics solution can be used to establish full-spectrum maritime domain awareness in any coastal waters.

Differentiating Traffic

For example, it can help operators differentiate between busy small vessel traffic and the traffic of larger vessels in coastal regions and in near proximity to oil rigs and oil tankers. For this type of application, the solution can be configured to track and view only those vessels of interest by first establishing a geographic fence around accepted trade lanes for vessels of a specific type or tonnage (Figure 3).

Figure 3: Creating a geographic fence along routine trade lanes.



Name: Non Conventional

Description: Non Conventional Shipping Zone

Search: 3 vessel types

☑ Link to Rule

Default Score: 5

● Polygon ○ Circle

Latitude:

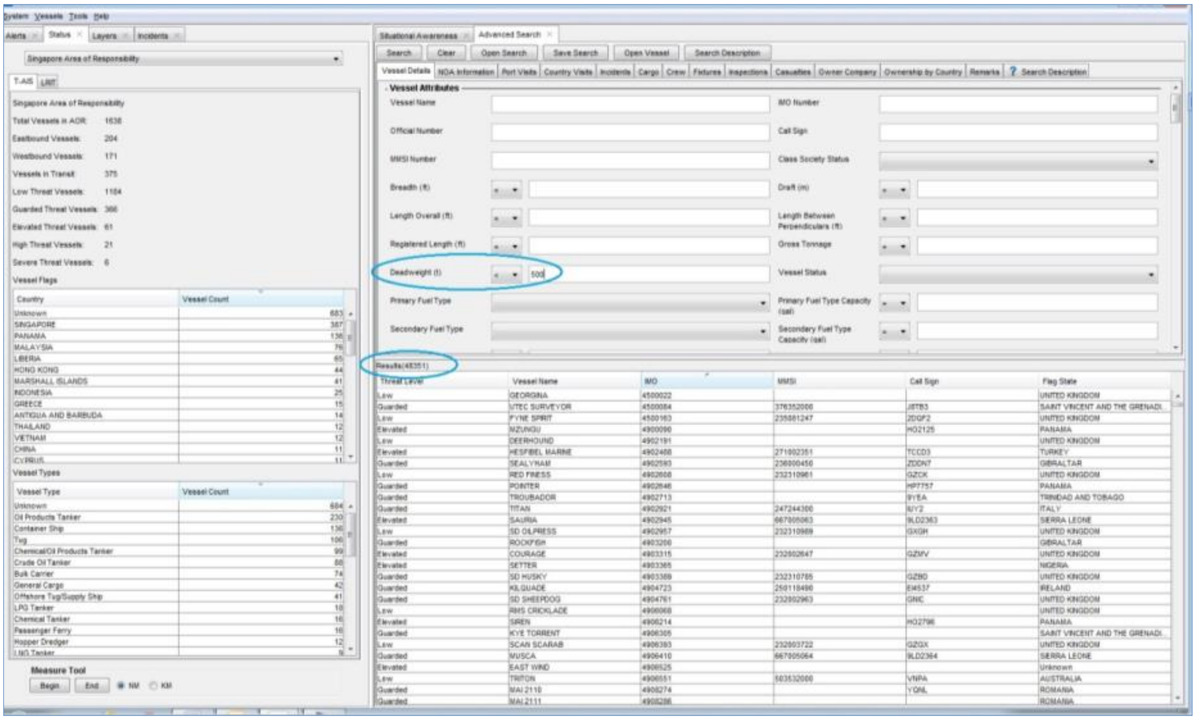
Longitude:

Coordinates:

(5.4223°, 115.3673°)
(6.1033°, 116.0525°)
(6.4446°, 115.6175°)
(4.9602°, 114.0322°)
(4.6466°, 114.3055°)
(5.0410°, 114.9795°)
(5.4223°, 115.3673°)

Once the fence is established, the system can be instructed to search for ships under 500 tons (Figure 4). The search criteria can be saved as a rule that triggers when a non-IMO and non-AIS surface target enters the area. Any targets are identified using Radio Frequency (RF) intercept sensor and/or via a radar signature and/or via satellite Synthetic Aperture Radar (SAR) signals parsed by the Rapid Technology Integration Framework (RTIF) Adapter.

Figure 4: Search criteria can be established for vessels of interest.


System Vessels Tools Help
Alerts Status Layers Incidents
Singapore Area of Responsibility
T-AIS LRIT
Situational Awareness Advanced Search
Search Clear Open Search Save Search Open Vessel Search Description
Vessel Details NOA Information Port Visits Country Visits Incidents Cargo Crew Fixtures Inspections Casualties Owner Company Ownership by Country Remarks ? Search Description
Measure Tool
Begin End ● NM ○ KM

Singapore Area of Responsibility
Total Vessels in AOR: 1638
Eastbound Vessels: 204
Westbound Vessels: 171
Vessels in Transit: 375
Low Threat Vessels: 1184
Guarded Threat Vessels: 366
Elevated Threat Vessels: 61
High Threat Vessels: 21
Severe Threat Vessels: 6

Vessel Flags

Country	Vessel Count
Unknown	683
SINGAPORE	387
PANAMA	136
MALAYSIA	76
LIBERIA	65
HONG KONG	44
MARSHALL ISLANDS	41
INDONESIA	25
GREECE	15
ANTIGUA AND BARBUDA	14
THAILAND	12
VIETNAM	12
CHINA	11
CYPRUS	11

Vessel Types

Vessel Type	Vessel Count
Unknown	684
Oil Products Tanker	230
Container Ship	136
Tug	106
Chemical/Oil Products Tanker	99
Crude Oil Tanker	88
Bulk Carrier	74
General Cargo	42
Offshore Tug/Supply Ship	41
LPG Tanker	18
Chemical Tanker	16
Passenger Ferry	16
Hopper Dredger	12
LNG Tanker	9

Vessel Attributes

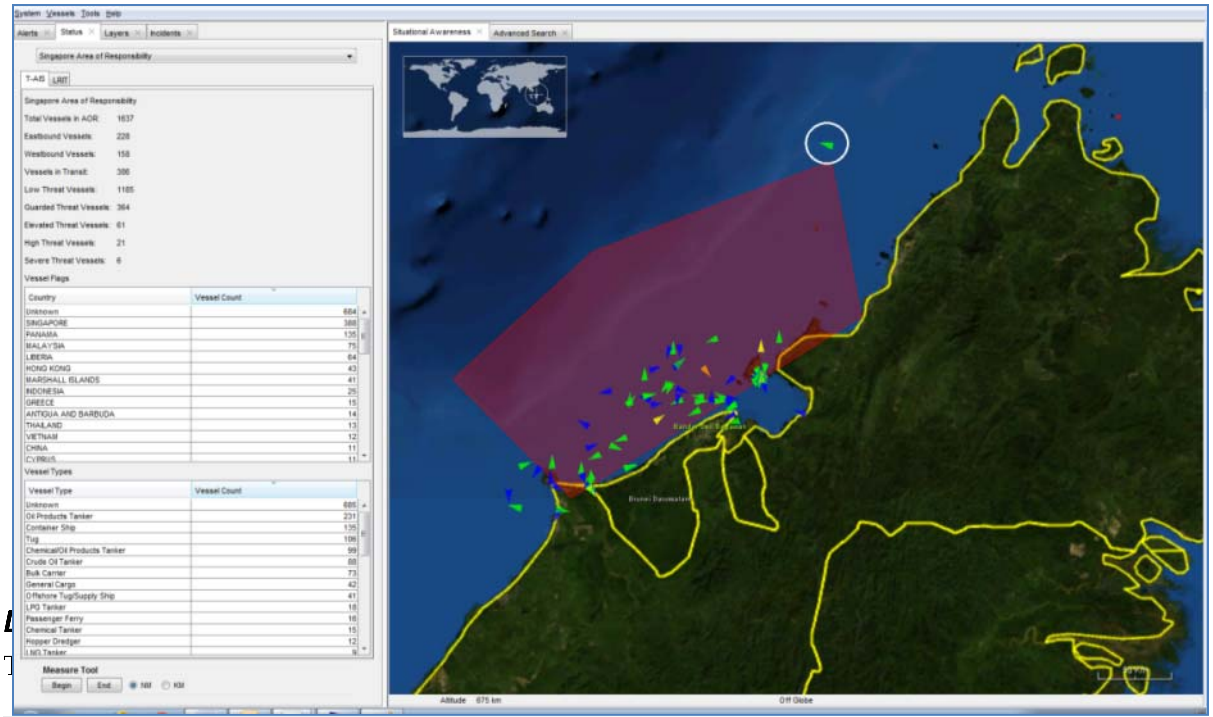
Vessel Name		IMO Number	
Official Number		Call Sign	
MMSI Number		Class Society Status	
Breadth (ft)	=	Draft (m)	=
Length Overall (ft)	=	Length Between Perpendiculars (ft)	=
Registered Length (ft)	=	Gross Tonnage	=
Deadweight (t)	< 500	Vessel Status	
Primary Fuel Type		Primary Fuel Type Capacity (gal)	=
Secondary Fuel Type		Secondary Fuel Type Capacity (gal)	=

Results(45351)

Threat Level	Vessel Name	IMO	MMSI	Call Sign	Flag State
Low	GEORGINA	4500022			UNITED KINGDOM
Guarded	UTEC SURVEYOR	4500084	376352000	J8TB3	SAINT VINCENT AND THE GRENADI
Low	FYNE SPIRIT	4500163	235881247	2DQF2	UNITED KINGDOM
Elevated	MZUNGU	4900090		HO2125	PANAMA
Low	DEERHOUND	4902191			UNITED KINGDOM
Elevated	HESPIBEL MARINE	4902468	271002351	TCCD3	TURKEY
Guarded	SEALYHAM	4902593	236000450	ZDDN7	GIBRALTAR
Low	RED FINESS	4902608	232310961	GZCK	UNITED KINGDOM
Guarded	POINTER	4902646		HP7757	PANAMA
Guarded	TROUBADOR	4902713		9YEA	TRINIDAD AND TOBAGO
Guarded	TITAN	4902921	247244300	IUY2	ITALY
Elevated	SAURIA	4902945	667005063	9LD2363	SIERRA LEONE
Low	SD OILPRESS	4902957	232310989	GXGH	UNITED KINGDOM
Guarded	ROCKFISH	4903200			GIBRALTAR
Elevated	COURAGE	4903315	232002647	GZMV	UNITED KINGDOM
Elevated	SETTER	4903365			NIGERIA
Guarded	SD HUSKY	4903389	232310785	GZBD	UNITED KINGDOM
Guarded	KILQUADE	4904723	250118490	EI4537	IRELAND
Guarded	SD SHEEPDOG	4904761	232002963	GNIC	UNITED KINGDOM
Low	RMS CRICKLADE	4906068			UNITED KINGDOM
Elevated	SIREN	4906214		HO2798	PANAMA
Guarded	KYE TORRENT	4906305			SAINT VINCENT AND THE GRENADI
Low	SCAN SCARAB	4906393	232003722	GZGX	UNITED KINGDOM
Guarded	MUSCA	4906410	667005064	9LD2364	SIERRA LEONE
Elevated	EAST WIND	4906525			Unknown
Low	TRITON	4906551	503532000	VNPA	AUSTRALIA
Guarded	MAI 2110	4908274		YQNL	ROMANIA
Guarded	MAI 2111	4908286			ROMANIA

If a subject target exits in the established geographic fence, then an event is logged and the pre-designated authority alerted (Figure 5).

Figure 5: Targets are identified in the geographic fence based on pre-defined search parameters.


System Vessels Tools Help
Alerts Status Layers Incidents
Singapore Area of Responsibility
T-AIS LRIT
Situational Awareness Advanced Search
Bandar Seri Begawan
Brunei Darussalam
Altitude 675 km
Off Globe
Measure Tool
Begin End ● NM ○ KM

Singapore Area of Responsibility
Total Vessels in AOR: 1637
Eastbound Vessels: 228
Westbound Vessels: 158
Vessels in Transit: 386
Low Threat Vessels: 1185
Guarded Threat Vessels: 364
Elevated Threat Vessels: 61
High Threat Vessels: 21
Severe Threat Vessels: 6

Vessel Flags

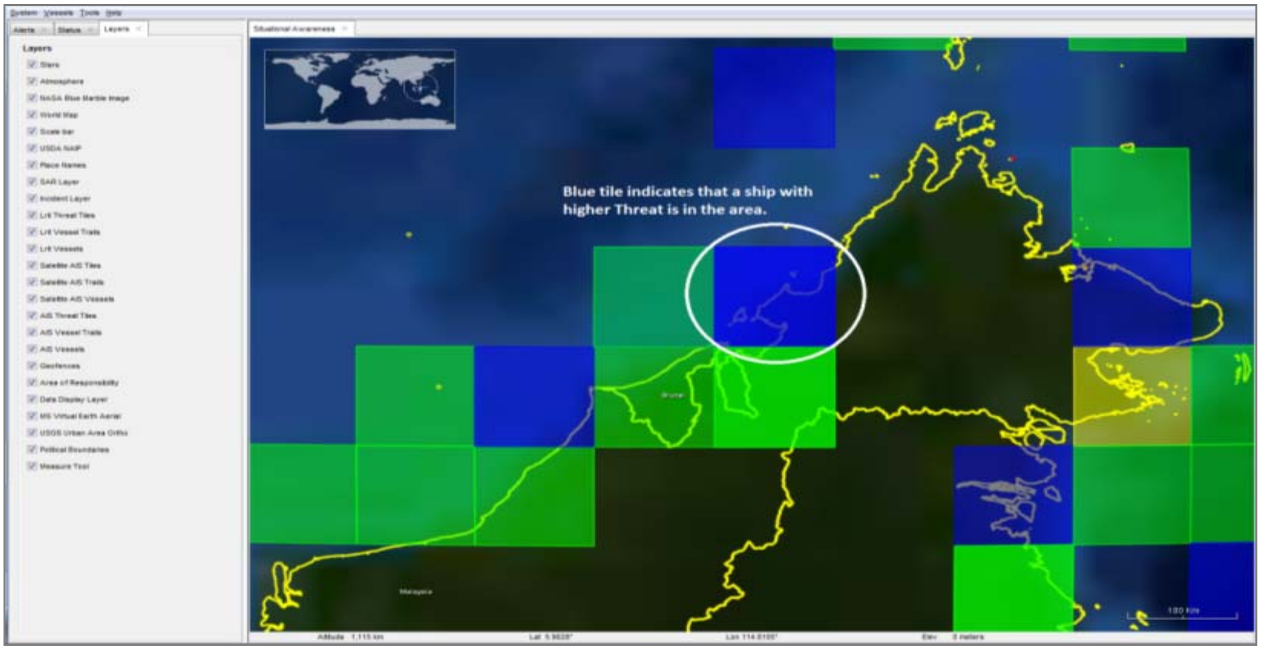
Country	Vessel Count
Unknown	684
SINGAPORE	388
PANAMA	135
MALAYSIA	75
LIBERIA	64
HONG KONG	43
MARSHALL ISLANDS	41
INDONESIA	25
GREECE	15
ANTIGUA AND BARBUDA	14
THAILAND	13
VIETNAM	12
CHINA	11
CYPRUS	11

Vessel Types

Vessel Type	Vessel Count
Unknown	685
Oil Products Tanker	231
Container Ship	135
Tug	106
Chemical/Oil Products Tanker	99
Crude Oil Tanker	88
Bulk Carrier	73
General Cargo	42
Offshore Tug/Supply Ship	41
LPG Tanker	18
Passenger Ferry	16
Chemical Tanker	15
Hopper Dredger	12
LNG Tanker	9

For example, the arrival of a potential oil smuggling ship may indicate that the ship intends to steal some oil. To secure assets against such activity, the system can be pre-configured to alert operators about any high-risk ships entering a specific area (Figure 6).

Figure 6: The system alerts the operator that a high risk ship has entered the area.

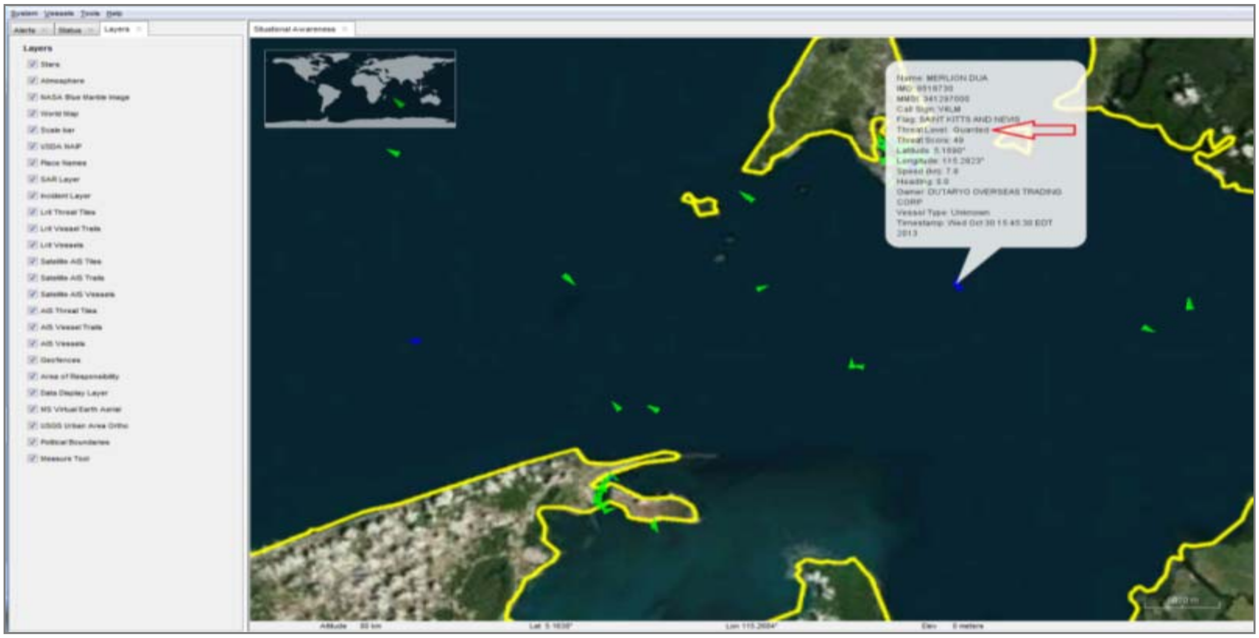


Layers
- ☑ Stars
- ☑ Atmosphere
- ☑ NASA Blue Marble Image
- ☑ World Map
- ☑ Scale bar
- ☑ USDA NAIP
- ☑ Place Names
- ☑ SAR Layer
- ☑ Incident Layer
- ☑ LrIt Threat Tiles
- ☑ LrIt Vessel Trails
- ☑ LrIt Vessels
- ☑ Satellite AIS Tiles
- ☑ Satellite AIS Trails
- ☑ Satellite AIS Vessels
- ☑ AIS Threat Tiles
- ☑ AIS Vessel Trails
- ☑ AIS Vessels
- ☑ Geofences
- ☑ Area of Responsibility
- ☑ Data Display Layer
- ☑ MS Virtual Earth Aerial
- ☑ USGS Urban Area Ortho
- ☑ Political Boundaries
- ☑ Measure Tool

Blue tile indicates that a ship with higher Threat is in the area.

Once alerted, an operator can leverage the full-featured information analysis utilities to pinpoint the high-risk vessel and identify it (Figure 7).

Figure 7: An operator can pinpoint high-risk targets.

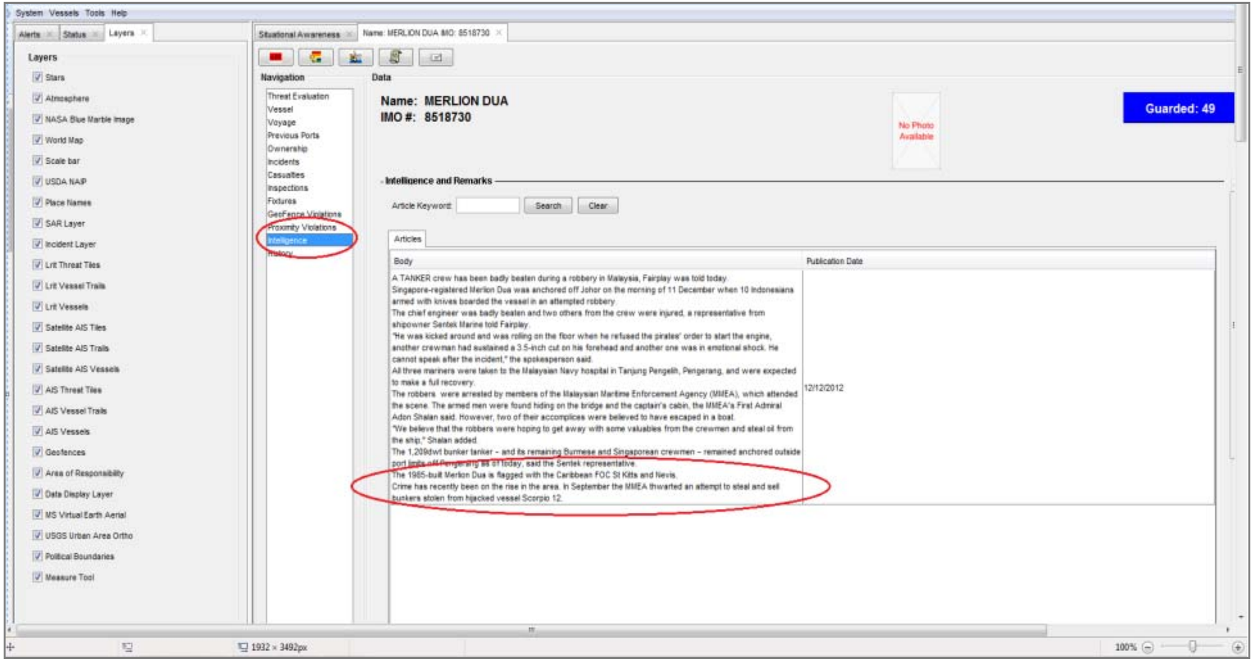


Layers
- ☑ Stars
- ☑ Atmosphere
- ☑ NASA Blue Marble Image
- ☑ World Map
- ☑ Scale bar
- ☑ USDA NAIP
- ☑ Place Names
- ☑ SAR Layer
- ☑ Incident Layer
- ☑ LrIt Threat Tiles
- ☑ LrIt Vessel Trails
- ☑ LrIt Vessels
- ☑ Satellite AIS Tiles
- ☑ Satellite AIS Trails
- ☑ Satellite AIS Vessels
- ☑ AIS Threat Tiles
- ☑ AIS Vessel Trails
- ☑ AIS Vessels
- ☑ Geofences
- ☑ Area of Responsibility
- ☑ Data Display Layer
- ☑ MS Virtual Earth Aerial
- ☑ USGS Urban Area Ortho
- ☑ Political Boundaries
- ☑ Measure Tool

Name: MERLION DUA
IMO: 9518730
MMSI: 341297000
Call Sign: V4LM
Flag: SAINT KITTS AND NEVIS
Threat Level: Guarded
Threat Score: 49
Latitude: 5.1690°
Longitude: 115.2823°
Speed (kn): 7.8
Heading: 5.0
Owner: DUTARYO OVERSEAS TRADING CORP
Vessel Type: Unknown
Timestamp: Wed Oct 30 15:45:30 EDT 2013

Because the system has access to a variety of information databases, the operator can then research the target in detail and review any information related to its participation in oil piracy (Figure 8).

Figure 8: Once a target is identified, the operator can research historical data.



Name: MERLION DUA
IMO #: 8518730

Body	Publication Date
A TANKER crew has been badly beaten during a robbery in Malaysia, Fairplay was told today. Singapore-registered Merlion Dua was anchored off Johor on the morning of 11 December when 10 Indonesians armed with knives boarded the vessel in an attempted robbery. The chief engineer was badly beaten and two others from the crew were injured, a representative from shipowner Sentek Marine told Fairplay. "He was kicked around and was rolling on the floor when he refused the pirates' order to start the engine, another crewman had sustained a 3.5-inch cut on his forehead and another one was in emotional shock. He cannot speak after the incident," the spokesperson said. All three mariners were taken to the Malaysian Navy hospital in Tanjung Pengelih, Pengerang, and were expected to make a full recovery. The robbers were arrested by members of the Malaysian Maritime Enforcement Agency (MMEA), which attended the scene. The armed men were found hiding on the bridge and the captain's cabin, the MMEA's First Admiral Adon Shalan said. However, two of their accomplices were believed to have escaped in a boat. "We believe that the robbers were hoping to get away with some valuables from the crewmen and steal oil from the ship," Shalan added. The 1,209dwt bunker tanker – and its remaining Burmese and Singaporean crewmen – remained anchored outside port limits off Pengerang as of today, said the Sentek representative. The 1985-built Merlion Dua is flagged with the Caribbean FOC St Kitts and Nevis. Crime has recently been on the rise in the area. In September the MMEA thwarted an attempt to steal and sell bunkers stolen from hijacked vessel Scorpio 12.	12/12/2012

1932 × 3492px

With this complete situational intelligence, maritime security commanders can determine an appropriate course of action that will neutralize any potential threat against maritime assets.

Enabled by the Rapid Technology Integration Framework (RTIF)

The powerful capabilities of the General Dynamics' maritime surveillance and security solution are enabled by a state-of-the-art integration framework, which allows users and third parties to easily add new functions and new interfaces to a CoCommand system. The CoCommand RTIF is based on best practices in service oriented architecture (SOA) technology. The modular structure of the framework provides comprehensive and flexible interoperability and data exchange between systems and allows rapid and easy integration of new and legacy capabilities as needed.

RTIF is implemented on an open source software technology stack, which is comprised of Apache ServiceMix, Apache ActiveMQ, Apache Camel and Apache CXF. Apache ServiceMix and Apache ActiveMQ provide the CoCommand service bus, which delivers a component and middleware framework for CoCommand services. The interoperability server hosts a collection of services, which perform domain-specific functions, such as message translation, data fusion, data aggregation, and policy implementation.

CoCommand is supplied with an Integration Development Kit (IDK). The CoCommand IDK is a collection of tools and documentation structured to give third parties guidance on how best to customize and extend the CoCommand system. With this kit, third parties can add new modules to the interoperability server and add new user interface elements to CoMotion as needed.

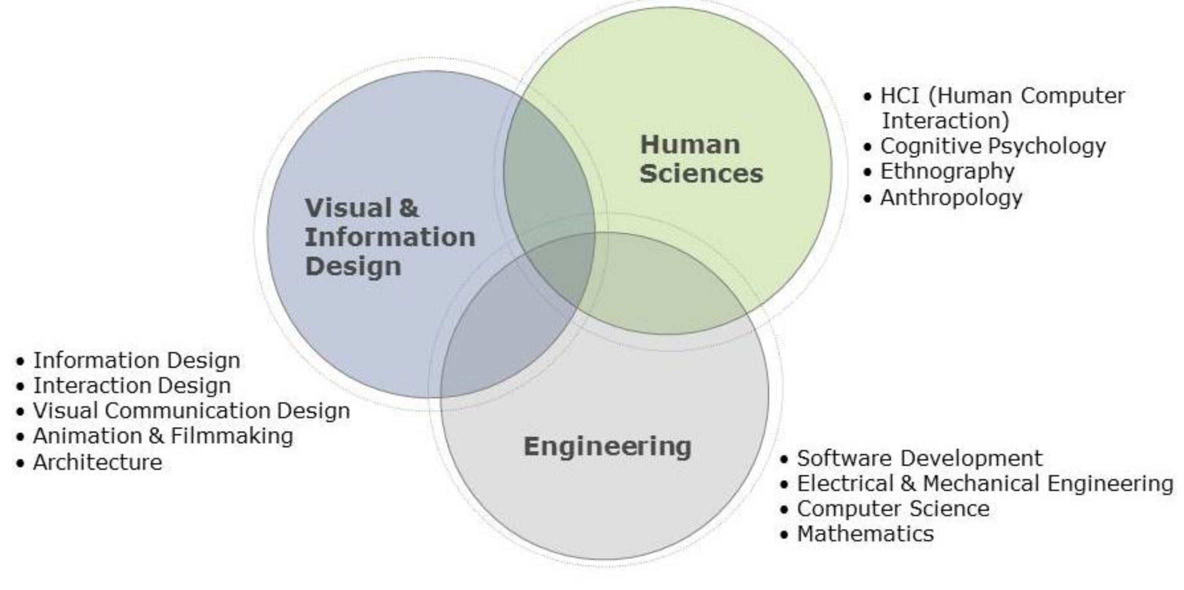
Built on Human-centered Design Criteria

Finally, to ensure the complete solution delivers maximum value during operations, CoCommand is engineered and developed based on HCD principles.

HCD is an interdisciplinary and iterative approach to design, focused on understanding and meeting human needs, rather than technology needs. It optimizes systems and user interfaces based on how people work, rather than forcing them to change how they work to accommodate the technology. To achieve this objective, an interdisciplinary HCD design team (Figure 9), which includes expertise in user and stakeholder research, as well as in traditional design and engineering disciplines, leverages the active involvement of users. This involvement includes the use of human research methods, such as task observations and interviews. The team uses this research to gain a clear understanding of user and task requirements, and then creates several iterations of a solution or partial solution to be tested with users until the ideal solution is developed.

With this approach, HCD ensures that technical constraints, visual design, and user requirements are always balanced against each other to create a more balanced and relevant end product. The result is an appropriate allocation of function between users and technology that allows people do the things they are good at and computers to do the work that they were designed for. Ultimately, this reduces the costs and risks associated with developing an integrated maritime surveillance system because it engages the end users in the process of identifying requirements that are often difficult to pin down and express in words.

Figure 9: CoCommand is engineered and developed based on HCD principles



Conclusion

CoCommand, the General Dynamics solution for efficient and effective maritime surveillance and security, enables security agencies to protect maritime assets and maintain complete security over coastal waters. It makes it easier for operators to track and filter traffic in any coastal water and view only those vessels of interest. This is achieved by streamlining the data collection process, aggregating massive amounts of data for analysis, and providing near real-time situational information to operators in an easily accessible and manageable format.

Armed with the right information, operators can quickly sift through all available data to identify targets of interest, define potential threats, and present a complete and accurate situational picture to commanders. With accurate situational awareness, commanders can weigh operational options, make assumptions, and estimate results. They can develop specific courses of action, if required, and initiate strategies that will ensure maritime security objectives are met. And they can make final decisions that can be easily communicated to all maritime agencies.

Ultimately, this improves the speed and accuracy of decisions at the strategic, tactical and operational levels of the command environment, and enables security agencies to establish full-spectrum domain awareness in all coastal waters.

Acronyms

Term	Definition
ACINT	acoustic intelligence
AIS	Automatic Identification System
COP	Common Operating Picture
HCD	human-centered design
HUMINT	human intelligence
IDK	Integration Development Kit
IMINT	imagery intelligence
IMO	International Maritime Organization
LRIT	Long Range Identification and Tracking
MASINT	measurement and signature intelligence
OSINT	open source intelligence
RADINT	radar intelligence
RAP	Recognized Air Picture
RCP	Recognized Cyber Picture
RF	Radio Frequency
RLP	Recognized Land Picture
RMP	Recognized Maritime Picture
ROSP	Recognized Operational Support Picture
RTIF	Rapid Technology Integration Framework
SAR	Synthetic Aperture Radar
SIGINT	signal intelligence
SLOC	Sea Line of Communications
SOA	Service Oriented Architecture