CENJOWS

ISSUE BRIEF
IB/52/26

TOWARDS A NATIONAL MARITIME TECHNOLOGY AND INTELLIGENCE CENTRE FOR INDIA

LT COL MANISH KOKEL (RETD)

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Towards a National Maritime Technology and Intelligence Centre for India

Lt Col Manish Kokel (Retd) is a serving as the Principal Consultant (IT) with the National e-Governance Division (NeGD) under Ministry of electronics and information technology (Meity)

Abstract

Maritime Domain Awareness (MDA) is emerging as the defining enabler of maritime power in the twenty-first century. For India, whose geopolitical and economic interests are deeply tied to the Indian Ocean Region (IOR), maritime security increasingly depends not merely on naval platforms but on the ability to generate persistent, predictive and network-centric awareness across the maritime battlespace. India has developed a substantial MDA framework through the Information Management and Analysis Centre (IMAC), the National Command, Control, Communication and Intelligence (NC3I) network, the Information Fusion Centre–Indian Ocean Region (IFC-IOR), coastal radar chains, Automatic Identification System (AIS) networks and indigenous maritime intelligence platforms.[1] However, the evolving threat environment—including dark shipping, cyber-attacks, grey-zone warfare, underwater threats and drone-enabled maritime terrorism—demands a transition from surveillance-centric systems towards AI-enabled, quantum-ready maritime intelligence architectures. This paper analyses India's existing MDA ecosystem, identifies its structural and technological limitations, compares it with advanced global systems and proposes the establishment of a National Maritime Technology and Intelligence Centre (NMTIC). The paper argues that India's future maritime dominance will depend upon integrating Artificial Intelligence (AI), satellite Intelligence, Surveillance and Reconnaissance (ISR) capabilities,

cyber resilience, Satellite Communication (SATCOM) interception, quantum communication and the National Intelligence Grid (NATGRID) feed into a unified Maritime Intelligence Grid capable of delivering decision superiority across the Indo-Pacific.

Strategic Context and Current Challenges

Introduction

The maritime domain has evolved from a physical battlespace into a multidimensional information environment encompassing surface, underwater, aerial, cyber, electromagnetic and space dimensions. India's maritime security environment is increasingly shaped by strategic competition in the Indo-Pacific, expanding Chinese naval presence in the IOR, maritime terrorism, illegal fishing, undersea infrastructure vulnerabilities and grey-zone operations. The majority of India's trade by volume transits through maritime routes,[2] making uninterrupted maritime awareness central to national security and economic resilience.

Reforms undertaken after the 26/11 Mumbai attacks fundamentally transformed India's coastal security architecture.[3] As noted by Captain Himadri Das, India developed a layered MDA framework integrating coastal radars, AIS systems, NC3I networks, IMAC and IFC-IOR.[4] These initiatives significantly improved maritime surveillance and inter-agency coordination. However, the contemporary threat environment now requires a paradigm shift from "awareness" towards "decision dominance." Future maritime warfare will increasingly depend upon which state can fuse diverse sensor inputs, intelligence feeds and predictive analytics faster than its adversaries.

India, therefore, needs a quantum-ready maritime intelligence grid integrating artificial intelligence, satellite Intelligence, Surveillance and Reconnaissance (ISR) capabilities, cyber intelligence, Signals Intelligence (SIGINT), Unmanned Aerial Vehicles (UAVs), the National Intelligence Grid (NATGRID) and quantum-secure communication into a unified operational architecture.

This paper adopts a qualitative strategic-analysis methodology based upon doctrinal review, open-source intelligence literature, maritime technology studies and comparative analysis of emerging maritime security architectures in the Indo-Pacific. The pa-

per additionally incorporates conceptual technology modelling and institutional capability assessment to propose an integrated Indian maritime intelligence grid architecture.

Existing Maritime Domain Awareness (MDA) Architecture

India's existing MDA ecosystem represents one of the most sophisticated maritime surveillance architectures in the Indian Ocean Region.[5] The Indian Navy operates the Information Management and Analysis Centre (IMAC), which functions as the central fusion hub for maritime information.[6] The NC3I (National Command, Control, Communication and Intelligence) Network is a highly secure communication backbone for India's maritime security. It interconnects naval and coastguard nodes, enabling near real-time maritime situational awareness.

India's Coastal Surveillance Network integrates radar stations, AIS receivers, electro-optical sensors and vessel traffic systems deployed along the coastline and island territories. Satellite capabilities, including Radar Imaging Satellite (RISAT), CARTOSAT, OCEANSAT and Electromagnetic Intelligence Satellite (EMISAT), further enhance Intelligence, Surveillance and Reconnaissance (ISR) capability. The Information Fusion Centre–Indian Ocean Region (IFC-IOR) extends this architecture into multinational maritime cooperation with liaison officers and linkages across more than 65 international partners.[7]

The DRDO's Centre for Artificial Intelligence and Robotics has additionally developed AI-enabled maritime situational systems such as Trigun and IMSAS,[8] integrating geospatial analytics, multi-sensor fusion and AI-assisted mission planning. These developments reflect India's gradual transition towards network-centric maritime warfare.

Nevertheless, India's MDA architecture remains distributed across multiple agencies and lacks unified integration of cyber intelligence, signals intelligence, predictive AI systems and quantum-resilient communication frameworks.

Emerging Threat Environment

The future maritime threat spectrum is increasingly characterised by ambiguity, deception and distributed warfare. Traditional radar and AIS-based systems are insuffi-

cient against dark ships, spoofed AIS signatures, autonomous systems and non-co-operative actors. Remote sensing intelligence studies demonstrate that adversaries increasingly employ Global Navigation Satellite System (GNSS) manipulation, AIS spoofing and deceptive routing to evade conventional maritime surveillance.[9]

Underwater threats also represent a growing challenge. Semi-submersibles, underwater drones and potential sabotage of undersea communication cables have introduced an entirely new dimension of maritime vulnerability.[10] Simultaneously, drone-enabled attacks against ports, offshore platforms and coastal infrastructure demonstrate the expanding aerial dimension of maritime threats.

Cyber-attacks against ports & maritime logistics systems have similarly emerged as strategic threats.[11] Modern ports depend heavily on Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, satellite navigation systems and interconnected digital logistics platforms. A coordinated cyber-attack against a major port could disrupt national supply chains without a single kinetic strike.

The maritime battlespace is therefore no longer purely naval; it is increasingly an integrated information warfare environment.

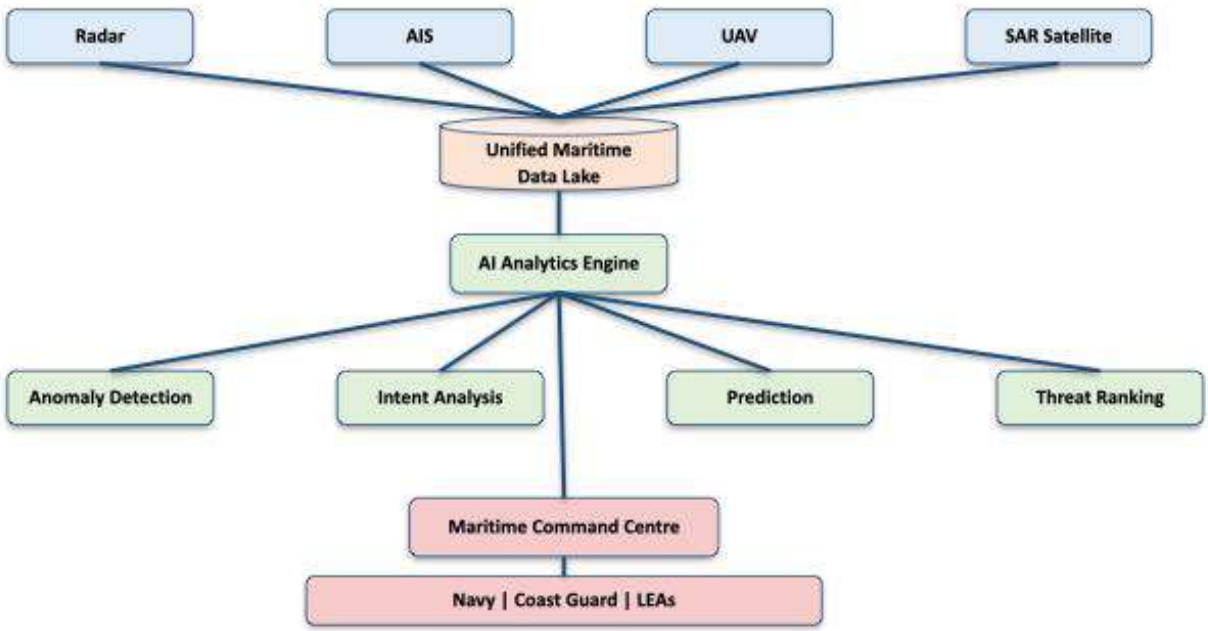

Figure 1: AI-Enabled Maritime Intelligence Architecture

AI-Enabled Maritime Intelligence

The future of maritime domain awareness lies in the development of Cognitive Maritime Intelligence Systems (CMIS) that combine artificial intelligence, machine learning, and multi-sensor fusion to transform vast volumes of maritime data into actionable intelligence.[12] Unlike traditional surveillance architectures that rely heavily on human interpretation, cognitive systems can continuously learn from operational patterns, correlate information across multiple domains, and identify anomalies that may otherwise remain undetected. Such capabilities enable predictive rather than reactive maritime security.

Future AI-enabled architectures should be capable of analysing vessel behaviour over extended periods to establish normal operational patterns and identify deviations that may indicate suspicious activity.[13] By correlating satellite imagery, Automatic Identification System (AIS) transmissions, radar tracks, communication metadata, and environmental information, these systems can assess vessel intent, generate dynamic risk scores, and prioritise threats in real time. This transition from object detection to intent assessment represents one of the most significant transformations in modern maritime intelligence.

AI Function	Operational Role	Strategic Impact
Behavioural Anomaly Detection	Detect unusual vessel movement	Dark shipping detection
Pattern-of-Life Analytics	Establish vessel behavioural baselines	Grey-zone activity identification
Vessel Intent Analysis	Predict likely operational intent	Early warning
Predictive Routing Models	Forecast vessel trajectory	Resource optimisation
Automated Threat Prioritisation	Rank threats dynamically	Faster operational response

Table 1: A modern AI-enabled MDA system should integrate five major analytical layers

The integration of artificial intelligence with remote sensing platforms further enhances maritime awareness by enabling simultaneous analysis of synthetic aperture radar (SAR) imagery, electro-optical feeds, radio-frequency (RF) emissions, oceanographic conditions, and shipping databases. Such fusion allows maritime authorities to identify deceptive behaviour, dark shipping activities, and grey-zone operations that may evade conventional surveillance mechanisms. As maritime competition increasingly shifts towards information-centric operations, AI-enabled intelligence architectures will become indispensable components of national maritime security systems. Such systems have been operationalised internationally.[14]

This creates a multi-dimensional intelligence environment capable of detecting deceptive maritime behaviour invisible to conventional systems.

Satcom Interception and SIGINT Integration

Signals Intelligence (SIGINT) and Satellite Communication (SATCOM) interception are emerging as critical pillars of future Maritime Domain Awareness architectures.[15] While conventional surveillance systems remain effective for monitoring cooperative maritime traffic, they provide only limited insight into the intentions, coordination patterns, and communication networks of non-cooperative actors. The growing prevalence of grey-zone operations, maritime terrorism, illegal fishing networks, and covert logistics chains necessitates a deeper understanding of the electromagnetic environment in which maritime activities occur.

Capability	Traditional ISR	ISR + SIGINT Fusion
Vessel Detection	Yes	Yes
Intent Assessment	Limited	Advanced
Communication Mapping	No	Yes
Grey-Zone Identification	Weak	Strong
Predictive Intelligence	Moderate	High

Table 2: ISR vs ISR+SIGINT Fusion

India possesses significant intelligence-gathering capabilities through institutions such as National Technical Research Organisation (NTRO), EMISAT, the Multi Agency Centre (MAC), and various defence SIGINT organisations. However, these capabilities remain only partially integrated with operational maritime awareness systems. Future maritime intelligence architectures should therefore seek to combine traditional ISR capabilities with communication analysis, RF spectrum monitoring, signal geolocation, and electronic emissions tracking. Such integration would significantly improve the ability to detect suspicious communication patterns, identify covert networks, and anticipate emerging threats before they become operationally visible.[16]

The fusion of ISR and SIGINT data would also strengthen predictive intelligence capabilities by enabling analysts to correlate vessel movements with communication activity, financial networks, logistics chains, and other indicators of organised maritime activity.[17] In this sense, maritime intelligence would evolve from a surveillance-centric model towards a comprehensive intelligence-led framework capable of supporting strategic decision-making across the entire maritime domain.

Global Comparisons

Leading maritime powers such as the United States and China increasingly integrate RF intelligence and maritime SIGINT into their operational awareness architectures. Developing similar capabilities will be essential for India to address emerging maritime security challenges and close a critical gap in future maritime intelligence and operational decision-making.

India currently lacks a dedicated operational architecture integrating maritime SIGINT, cyber intelligence, satellite RF analytics and naval operational systems. This remains one of the most significant future capability gaps.

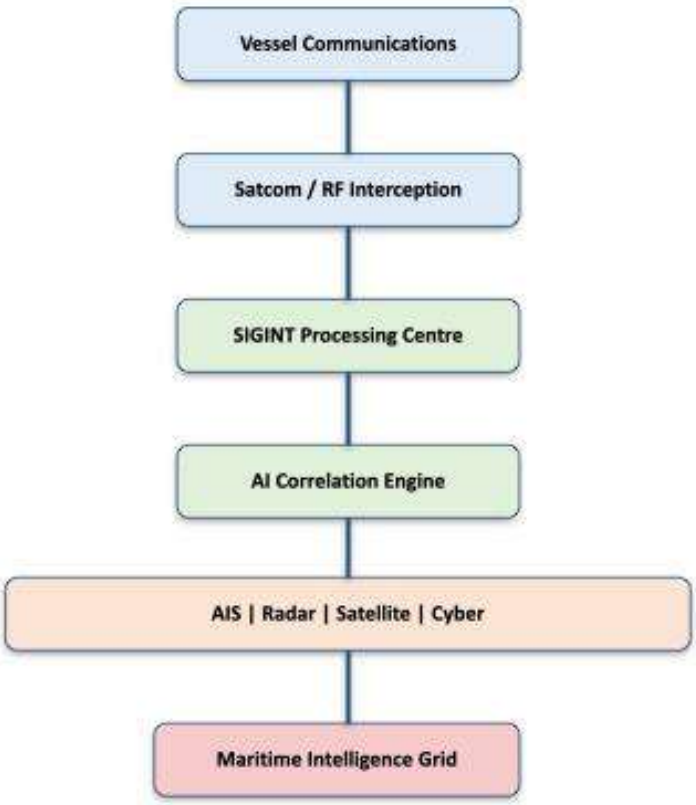

Figure 2: SIGINT-Integrated Maritime Awareness

Quantum Technologies and Maritime Security

Quantum technologies are poised to transform maritime security in much the same way that radar and satellite systems revolutionised naval operations in the twentieth century.[18] Their emergence presents both opportunities and challenges, particularly in the domains of secure communications, navigation, encryption and underwater warfare.

A key application is Quantum Key Distribution (QKD), which enables highly secure communication based on the principles of quantum physics.[19] Potential maritime applications include naval fleet communications, submarine networks, secure ISR data transmission and satellite-to-ship communication links. As major powers advance quantum communication capabilities, India must accelerate the development of quantum-secure maritime communication and command networks.

Quantum sensing represents another potentially transformative capability. Advanced quantum sensors may significantly enhance underwater domain awareness through

improved magnetic, gravimetric and navigation accuracy.[20] Such technologies could improve submarine detection, underwater tracking and anti-submarine warfare effectiveness, particularly in strategically important regions such as the Indian Ocean.

Although India possesses considerable quantum research expertise through national defence, space and academic institutions, maritime-specific quantum integration remains at an early stage. Developing dedicated quantum-enabled maritime programmes will be essential to maintaining future naval and maritime security competitiveness. A comparison amongst advanced militaries in this regard is given in the table below.

Country	Quantum Maritime Capability
China	Operational QKD demonstrations
USA	Advanced quantum sensing research
UK	Naval quantum navigation research
India	Emerging research stage

Table 3: Quantum Maritime Competition

Proposed National Maritime Technology and Intelligence Centre (NMTIC)

The Need for NMTIC

India has developed significant capabilities in maritime surveillance, intelligence gathering, space-based observation, defence electronics, artificial intelligence and cybersecurity. These capabilities are currently distributed across multiple organisations, including the Indian Navy, DRDO, ISRO, BEL, NTRO and various academic institutions. While each organisation contributes substantially within its respective domain, the absence of a common institutional framework limits the integration of technologies, intelligence, research, training and operational innovation required for future maritime security challenges.[21]

To address this gap, this paper proposes the establishment of a National Maritime Technology and Intelligence Centre (NMTIC) as a national-level centre of excellence for maritime technology, intelligence integration and capability development. The

NMTIC should function as India's apex maritime innovation and intelligence institution, jointly operated by the Indian Navy, DRDO, ISRO, Bharat Electronics Limited (BEL), NTRO, maritime universities and leading technical institutes. The centre would serve as a common platform for technology development, intelligence fusion, operational experimentation, doctrine formulation and strategic research. Similar technology centres exist internationally.[22]

Core Functional Divisions

The NMTIC should comprise specialised divisions dedicated to Maritime AI and Analytics, ISR Integration, SIGINT and SATCOM Intelligence, Maritime Cyber Defence, Quantum Technologies and Maritime Simulation and Wargaming. These divisions would collectively support the development of advanced Maritime Domain Awareness capabilities while fostering collaboration among defence, intelligence, industry and academic stakeholders.

Division	Core Role
Maritime AI & Analytics Lab	AI-enabled MDA systems
Quantum Communication Centre	QKD and quantum security
Maritime Cyber Defence Division	Port and maritime cyber resilience
SIGINT & RF Analytics Lab	Satcom interception integration
Digital Twin Simulation Centre	Maritime operational simulation
ISR Fusion Lab	Multi-domain intelligence fusion

Table 5: Core Functional Divisions of NMTIC

In addition to technology development, the centre should act as a national hub for talent development, multidisciplinary training, strategic studies and operational innovation. By integrating emerging technologies such as artificial intelligence, quantum communications, cyber intelligence, digital simulation and advanced ISR systems

within a single institutional framework, the NMTIC would provide India with a sustainable pathway towards maritime intelligence dominance and information superiority in the Indian Ocean Region.

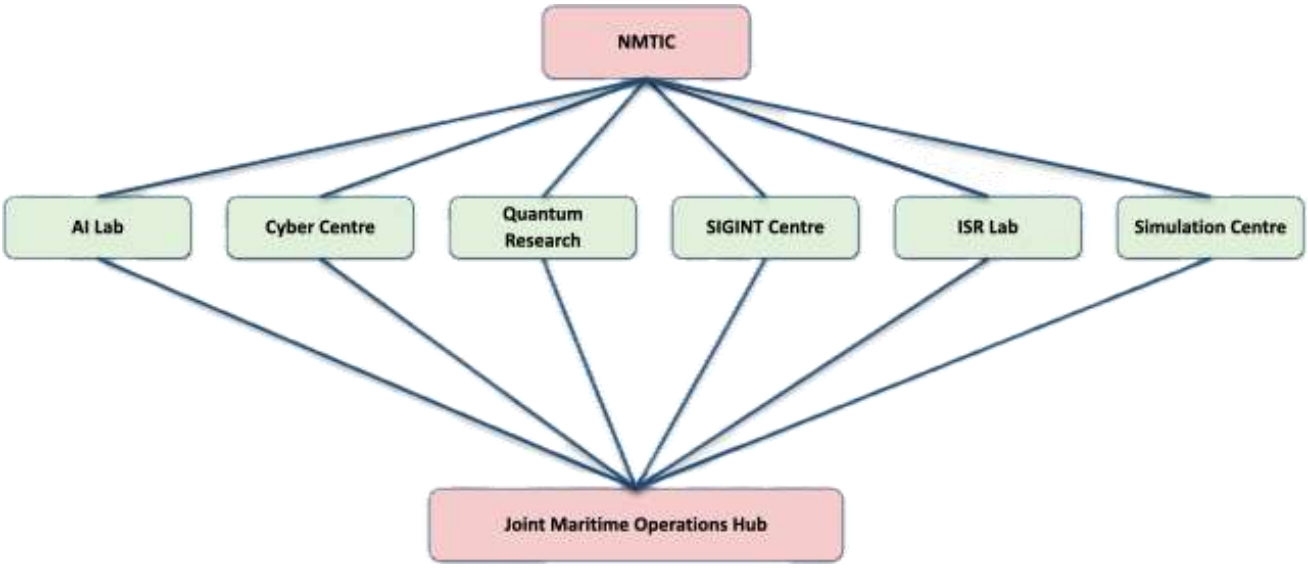

Figure 3: Proposed NMTIC Structure

Maritime Intelligence and Wargaming Environment (MIWE)

It is proposed that a Maritime Intelligence and Wargaming Environment (MIWE) be established at the NMTTIC, which could serve as the principal simulation, experimentation and strategic decision-support platform within the National Maritime Technology and Intelligence Centre (NMTIC). Designed as a multi-domain maritime intelligence ecosystem, MIWE would integrate real-time and historical data from maritime surveillance systems, intelligence networks, cyber monitoring platforms, space assets and operational command systems to create a continuously evolving virtual representation of India's maritime security environment.

Unlike traditional naval wargaming systems that primarily focus on fleet manoeuvres and kinetic operations, MIWE would simulate the entire maritime battlespace, including surface, subsurface, aerial, cyber, electromagnetic, space, logistics and intelligence dimensions. The objective would be to enable predictive intelligence generation, strategic foresight, technology evaluation, operational planning and capability development within a unified simulation framework.

The primary objective of MIWE would be to support India's transition from surveillance-centric maritime security to intelligence-driven maritime dominance. Specifically, MIWE would enable Strategic maritime planning, Operational war-gaming, Intelligence analysis cum forecasting, multi-agency coordination exercises, AI model training cum validation, Maritime technology experimentation, Crisis management simulations, Doctrine development and Capability gap assessment.

Talent Development Framework

The success of a future Maritime Intelligence Grid will depend as much on human capital as on technological capability. India currently lacks a dedicated multidisciplinary ecosystem that combines maritime strategy, artificial intelligence, cybersecurity, SIGINT, space systems, data fusion, quantum communications and radio frequency (RF) engineering within a single educational and training framework. The proposed NMTIC should therefore function as a national centre for talent development, creating a new generation of maritime intelligence professionals capable of operating at the intersection of technology, intelligence and maritime operations.

Through specialised academic programmes, simulation-based learning, joint research initiatives and industry partnerships, the NMTIC can develop the technical expertise required to support next-generation maritime security architectures. Such an approach would strengthen India's long-term capacity to design, operate and continuously evolve advanced maritime intelligence systems.

Strategic Implications

The establishment of an AI-enabled, quantum-ready maritime intelligence grid under the NMTIC framework would represent a significant shift in India's maritime security paradigm. Rather than relying primarily on surveillance and platform-centric operations, future maritime effectiveness will increasingly depend upon information fusion, predictive analytics, cognitive decision-support systems, electromagnetic awareness and secure digital networks.

As maritime competition becomes increasingly data-driven and technology-intensive, the ability to integrate intelligence from multiple domains and transform it into action-

able insights will become a decisive strategic advantage. Nations that achieve superiority in maritime intelligence architectures are likely to shape the future balance of power in the Indian Ocean Region and the wider Indo-Pacific.

NATGRID and National Maritime Intelligence Fusion

The future effectiveness of India's maritime security architecture will increasingly depend upon the ability to integrate operational maritime awareness with broader national intelligence systems. NATGRID offers an important opportunity in this regard by providing a framework through which diverse datasets from multiple government agencies can be accessed and correlated for security purposes. Although originally conceived as a counter-terrorism platform following the 26/11 Mumbai attacks,[23] its underlying architecture has significant implications for maritime security.

Modern maritime threats rarely operate in isolation.[24] Illegal fishing syndicates, narcotics traffickers, sanctions-evasion networks, maritime terrorist organisations, and grey-zone actors frequently rely upon interconnected financial, communication, logistics, and transportation networks. By integrating NATGRID with IMAC, NC3I, IFC-IOR, and NTRO-supported intelligence systems, India could move beyond traditional vessel tracking towards comprehensive maritime network analysis. Suspicious vessel activity could be examined alongside telecommunications metadata, banking records, customs information, immigration databases, cargo manifests, and satellite communication patterns, thereby providing a much richer intelligence picture.

Such integration would transform Maritime Domain Awareness into a true Maritime Intelligence Fusion Architecture capable of identifying relationships, predicting threats, and supporting proactive security operations. When combined with artificial intelligence and advanced analytics, NATGRID-enabled maritime intelligence systems could provide unprecedented insight into the behaviour of complex maritime networks operating across physical, cyber, financial, and communication domains.

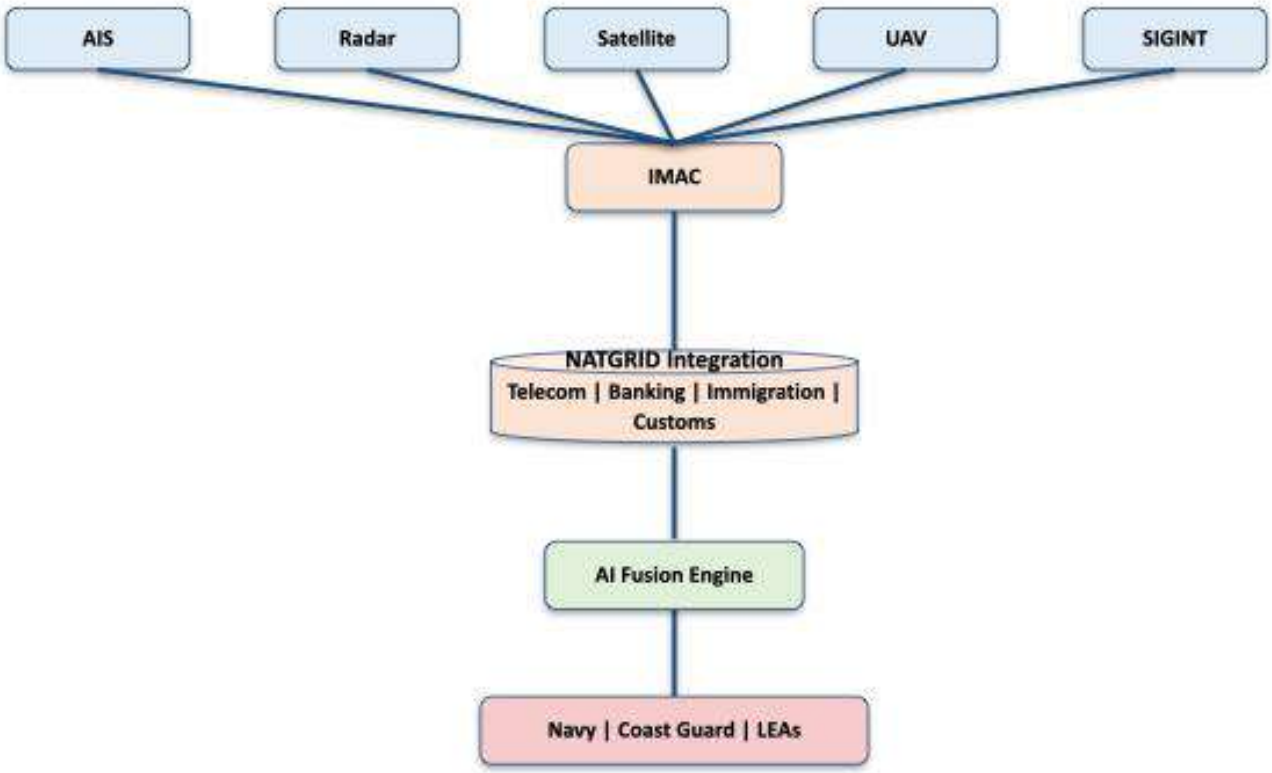

Figure 4: NATGRID-Enabled Maritime Intelligence Fusion

Conclusion

India's post-26/11 maritime reforms successfully created the foundational architecture for maritime surveillance and coordination. However, the future battlespace requires a transition from maritime surveillance to maritime intelligence dominance. AI-enabled ISR fusion, satcom interception, cyber resilience and quantum-secure communication must become central pillars of India's maritime strategy.

The proposed Quantum-Ready Maritime Intelligence Grid and National Maritime Technology and Intelligence Centre provide a roadmap for this transformation. In the coming decades, maritime power will increasingly belong not to states with the largest fleets, but to those capable of achieving superior information fusion, predictive awareness and decision dominance across the maritime domain.[25]

List of Abbreviations and Acronyms

These were used and/ or implied in the paper.

Abbreviation	Full Form
AI	Artificial Intelligence
AIS	Automatic Identification System
AIS-SB	Automatic Identification System – Space Based
API	Application Programming Interface
ASW	Anti-Submarine Warfare
BEL	Bharat Electronics Limited
CAIR	Centre for Artificial Intelligence and Robotics
CARTOSAT	Cartographic Satellite
CIBMS	Comprehensive Integrated Border Management System
CMIS	Cognitive Maritime Intelligence Systems
CNES	Centre National d'Études Spatiales (French Space Agency)
COP	Common Operating Picture
COPERNICUS	European Union Earth Observation Programme
CSN	Coastal Surveillance Network
DGLL	Directorate General of Lighthouses and Lightships
DG Shipping	Directorate General of Shipping
DRDO	Defence Research and Development Organisation
EEZ	Exclusive Economic Zone
EMISAT	Electronic Intelligence Satellite

Abbreviation	Full Form
EO	Electro-Optical
EU	European Union
GNSS	Global Navigation Satellite System
GRT	Gross Registered Tonnage
GSAT	Geostationary Satellite
IA	Artificial Intelligence
IACCS	Integrated Air Command and Control System
ICS	Industrial Control System
IDA	Information–Decision–Action
IFC-IOR	Information Fusion Centre – Indian Ocean Region
IFF	Identification Friend or Foe
IMAC	Information Management and Analysis Centre
IMO	International Maritime Organization
IMSAS	Integrated Maritime Situational Awareness System
IOR	Indian Ocean Region
IORIS	Indian Ocean Regional Information Sharing Platform
IoT	Internet of Things
IPOI	Indo-Pacific Oceans Initiative
IR	Infrared
ISR	Intelligence, Surveillance and Reconnaissance
ISRO	Indian Space Research Organisation
IUHDSS	Integrated Underwater Harbour Defence and Surveillance System

Abbreviation	Full Form
LRIT	Long-Range Identification and Tracking
MAC	Multi Agency Centre
MDA	Maritime Domain Awareness
MISTA	Maritime Information Sharing Technical Agreement
ML	Machine Learning
MoD	Ministry of Defence
MoU	Memorandum of Understanding
MPA	Maritime Patrol Aircraft
MSC	Maritime Safety Committee
MSIS	Merchant Ship Information System
NADS	Naval Anti-Drone System
NAIS	National Automatic Identification System
NATGRID	National Intelligence Grid
NC3I	National Command, Control, Communication and Intelligence
NMDAC	National Maritime Domain Awareness Centre
NMF	National Maritime Foundation
NMTIC	National Maritime Technology and Intelligence Centre
NSA	National Security Agency (USA)
NTCPWC	National Technology Centre for Ports, Waterways and Coasts
NTRO	National Technical Research Organisation
OECD	Organisation for Economic Co-operation and Development
OCEANSAT	Ocean Satellite

Abbreviation	Full Form
ONGC	Oil and Natural Gas Commission
PSC	Port State Control
QKD	Quantum Key Distribution
RF	Radio Frequency
RFMO	Regional Fisheries Management Organisation
RISAT	Radar Imaging Satellite
SAR	Synthetic Aperture Radar
SCADA	Supervisory Control and Data Acquisition
SHADE	Shared Awareness and Deconfliction
SIGINT	Signals Intelligence
SOP	Standard Operating Procedure
UAV	Unmanned Aerial Vehicle
UDA	Underwater Domain Awareness
US	United States
VATMS	Vessel and Air Traffic Management System
VIIRS	Visible Infrared Imaging Radiometer Suite
VTS	Vessel Traffic Service
VTMS	Vessel Traffic Management System
WSIE	White Shipping Information Exchange

Additional Abbreviations

These were conceptually used or implied in the paragraphs.

Abbreviation	Full Form
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CMDA	Cognitive Maritime Domain Awareness
EW	Electronic Warfare
ELINT	Electronic Intelligence
OSINT	Open-Source Intelligence
HUMINT	Human Intelligence
TECHINT	Technical Intelligence
GEOINT	Geospatial Intelligence
COMINT	Communications Intelligence
RFINT	Radio Frequency Intelligence
AIoT	Artificial Intelligence of Things
UUV	Unmanned Underwater Vehicle
USV	Unmanned Surface Vehicle
LEO	Low Earth Orbit
SATCOM	Satellite Communication
VUCA	Volatile, Uncertain, Complex and Ambiguous
QIS	Quantum Information Science
PNT	Positioning, Navigation and Timing
SOC	Security Operations Centre

Abbreviation	Full Form
SIEM	Security Information and Event Management
SOCMINT	Social Media Intelligence
MINT	Maritime Intelligence
CMF	Combined Maritime Forces
COPS	Common Operational Picture Systems

Declaration

I declare that this manuscript is being submitted exclusively to CENJOWS for publication consideration, is original, and has not been published or submitted elsewhere. I further certify that it contains no classified, restricted, or sensitive information and is based entirely on open-source material suitable for publication in the public domain.

ENDNOTES

[1]Indian Navy, Ensuring Secure Seas: Indian Maritime Security Strategy (New Delhi: Integrated Headquarters Ministry of Defence (Navy), 2015).

[2] Ministry of Ports, Shipping and Waterways, Maritime India Vision 2030 (New Delhi, 2021).

[3] Ministry of Home Affairs, Annual Report 2009–10.

[4] Himadri Das, Maritime Domain Awareness: Shifting Paradigms (New Delhi: National Maritime Foundation, 2021).

[5] Indian Navy, Ensuring Secure Seas.

[6] Information Management and Analysis Centre (IMAC), Indian Navy publications.

[7] IFC-IOR, Information Fusion Centre – Indian Ocean Region official publications.

[8] DRDO, Centre for Artificial Intelligence and Robotics publications.

[9] Windward, Remote Sensing Intelligence for Maritime Security (2023).

[10] OECD, Security of Submarine Cables, 2022.

[11] International Maritime Organization, Guidelines on Maritime Cyber Risk Management, 2021.

[12] NATO Centre for Maritime Research and Experimentation, Artificial Intelligence and Maritime Security, 2022.

[13] Windward, Remote Sensing Intelligence.

[14] United States Coast Guard, Illegal Fishing and Dark Shipping Reports.

[15] RAND Corporation, Maritime SIGINT and Intelligence Fusion, 2021.

[16] United States Navy, Electromagnetic Maneuver Warfare Strategy.

[17] NATO Maritime Command, ISR Integration Concepts, 2020.

[18] National Quantum Mission, Government of India, 2023.

[19] ISRO, Quantum Communication Demonstration Reports.

[20] Royal Navy, Quantum Navigation Research Program.

[21] Standing Committee on Defence, Government of India, Defence Modernisation Reports.

[22] U.S. Naval Postgraduate School, Maritime Security Innovation Ecosystems.

[23] Government of India, NATGRID Concept Paper.

[24] United Nations Office on Drugs and Crime, Transnational Maritime Crime Report.

[25] Geoffrey Till, Seapower: A Guide for the Twenty-First Century, 4th ed. (London: Routledge, 2018).