PKIA 2025

Directorate General of Shipping

Shri. Ravi Kumar M
SS-cum-Dy. Director General(Tech)

Maritime Meets Cryptography

Sailing the Digital Sea of Trust

The Twin Seas of Maritime Operations
Modern ships navigate both the physical sea and the digital sea of data, documents, and secure communications, necessitating a secure information infrastructure.

From Paperwork to Instant Digital Authentication
Twenty years ago, maritime operations were paperwork-intensive; today, digital signatures enable real-time authentication and global verification of ship documents.

Efficiency in Global Trade
Digital trust systems have dramatically reduced port clearance times—from weeks to minutes—streamlining global maritime commerce.

Cryptography as the Core Enabler
Public-key cryptography ensures data authenticity, integrity, and non-repudiation, forming the backbone of secure maritime communication and documentation.

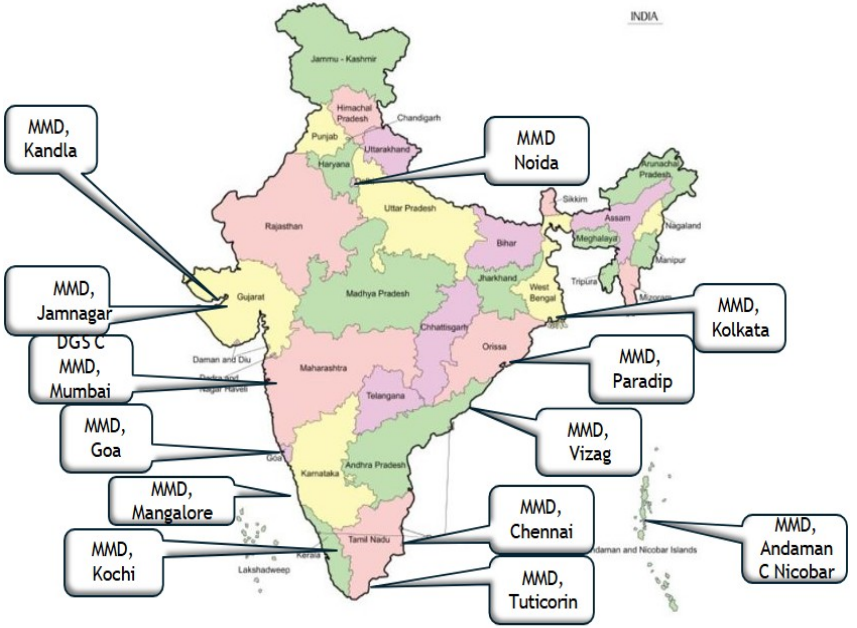
Directorate General of Shipping

- **Maritime Regulator under MoPSW**
  DG Shipping operates under the Ministry of Ports, Shipping & Waterways, implementing and enforcing maritime policy through the Merchant Shipping Act, 1958.

- **Safety, Pollution, and Seafarer Welfare**
  Ensures vessel safety, prevents marine pollution, oversees welfare and training standards for seafarers, and guarantees compliance with global conventions such as SOLAS, MARPOL, and STCW.

- **Training, Certification & Ship Inspection**
  Regulates maritime education, issues certifications like CoC, CDC, and SID, conducts Port State and Flag State inspections, and facilitates quality enforcement across MMDs.

- **International Representation & Legal Framework**
  Represents India in IMO and ILO forums, develops maritime policy, and ensures domestic alignment with global maritime laws and environmental standards.



Location of DGS & Mercantile Marine Departme

Indian Maritime Sector (Ports, Shipping & Waterways)

11,009 km long **Indian coastline** with **12 Major & 217 Non-major Ports**

Key components of Indian Maritime Sector

Ports

Ports	No. of ports	Cargo handled MMT (FY-24)
Major	12	818
Non-major	217	721

Shipping

Ship type	No. of Indian owned Ships (FY-23)	Capacity million GT (FY-23)
Coastal	1,039	1.7
Overseas	487	12.2
Total	1,526	13.8

Waterways

Number of Waterways	Cargo handled MMT (FY-24)
111	133

Source: Cargo handling status, April 2024, MoPSW; IWAI CAR-D

Cyber Threats in Maritime Sector

When Bits Fail, Ships Stop

NotPetya’s Global Disruption
The 2017 NotPetya ransomware crippled Maersk’s operations, halting cranes, trucks, and containers worldwide—including JNPT—resulting in $200–$300 million losses.

Ports Under Ransomware Siege
Major ports in South Africa (2021) and Japan (2023) were paralyzed by ransomware attacks, showing the sector's systemic vulnerabilities.

GPS Spoofing Threats
Incidents in the Black Sea involved 20 vessels reporting false locations, endangering navigational safety and security.

Operational Dependency on Digital
Digital failures directly disrupt physical operations—crane stoppages, delayed clearances, and stranded shipments amplify the need for cyber resilience.

Case : *"NotPetya"* Cyber Attack 2017 on MAERSK

Real World Scenario 2

- Back in June 2017, the global shipping giant Maersk Line, which handles nearly 20% of the world's container shipping, fell victim to a devastating cyberattack — **"NotPetya",** a malware originally targeting Ukrainian infrastructure..

Within hours, Maersk's global IT infrastructure was crippled:

- **Terminal operations halted** in major ports like Rotterdam, Mumbai, and Los Angeles.
- **Cargo tracking systems went offline**, leaving thousands of containers stranded.
- **Communication blackouts** occurred between ships and shore offices.
- The company had to **rebuild 4,000 servers and 45,000 PCs** from scratch

Over **$300 million** in losses

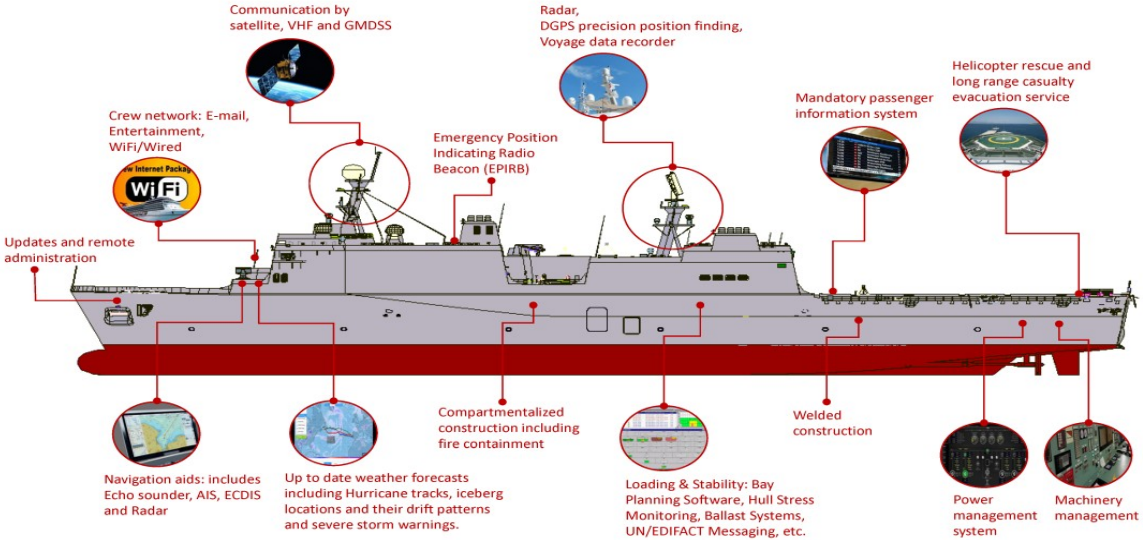
But here's the silver lining: Maersk's disaster recovery was aided by a single surviving domain controller in Ghana, a stroke of luck that allowed them to restore operations.

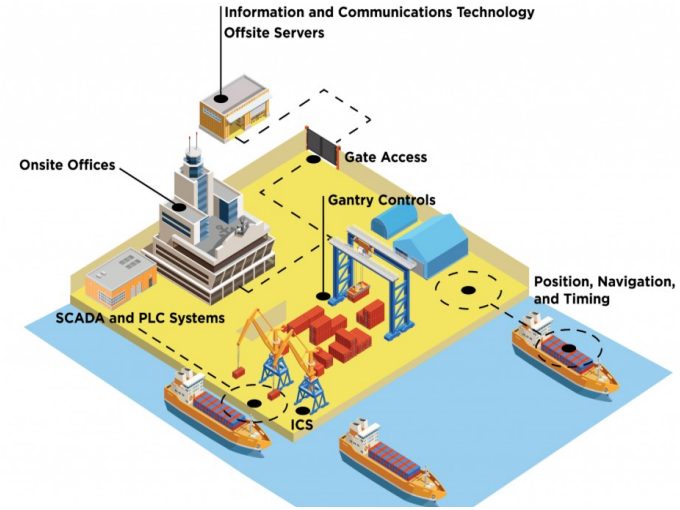
How DGS could be impacted from these threats

For an organization like DGS, which manages sensitive e-governance applications related to maritime operations, seafarer examinations, and compliance, such attacks could result in:

Enhancing Maritime Enforcement

Maritime Infrastructure:





Ship based

Shore based

- Increased interconnectedness with online systems, in turn make maritime infra more vulnerable to cyberattacks.

The 26/11 Turning Point

From Tragedy to Maritime Vigilance

The MV Kuber Incident

On November 26, 2008, terrorists hijacked the MV Kuber—a small fishing boat—used to infiltrate Mumbai undetected, resulting in a devastating attack with 166 deaths.

Exposure of Maritime Gaps

The incident revealed critical vulnerabilities in India’s maritime domain awareness—highlighting the lack of coastal surveillance and vessel identification systems.

Catalyst for Change

26/11 became the pivotal moment that spurred strategic investments into maritime tracking and national coastal defense.

Security Imperative Redefined

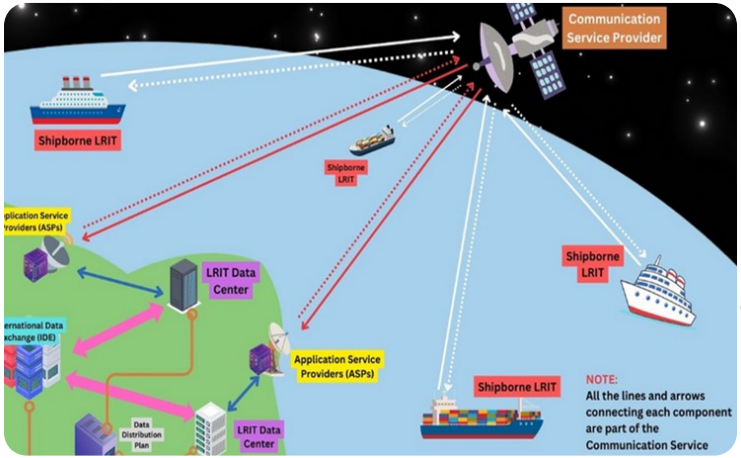
The tragedy reframed maritime security as a national priority, driving the development of long-range identification and tracking systems.

LRIT Capabilities & National Infrastructure

Encrypted Tracking for Sovereign Maritime Visibility

- **Genesis of LRIT System:** Post-26/11, India established the Long Range Identification and Tracking (LRIT) National Data Centre to enhance sovereign control over approaching vessels.
- **Real-Time Vessel Monitoring:** The LRIT Centre enables encrypted, real-time tracking of ships well beyond the coastal radar range, enhancing situational awareness.
- **Cryptography in Surveillance:** All data streams are secured using public-key infrastructure, ensuring integrity and authenticity of vessel position reports.
- **Maritime Domain Awareness Backbone:** LRIT has become a central pillar in India's maritime security apparatus, closing critical gaps in coastal monitoring.

LRIT (LONG-RANGE IDENTIFICATION AND TRACKING)

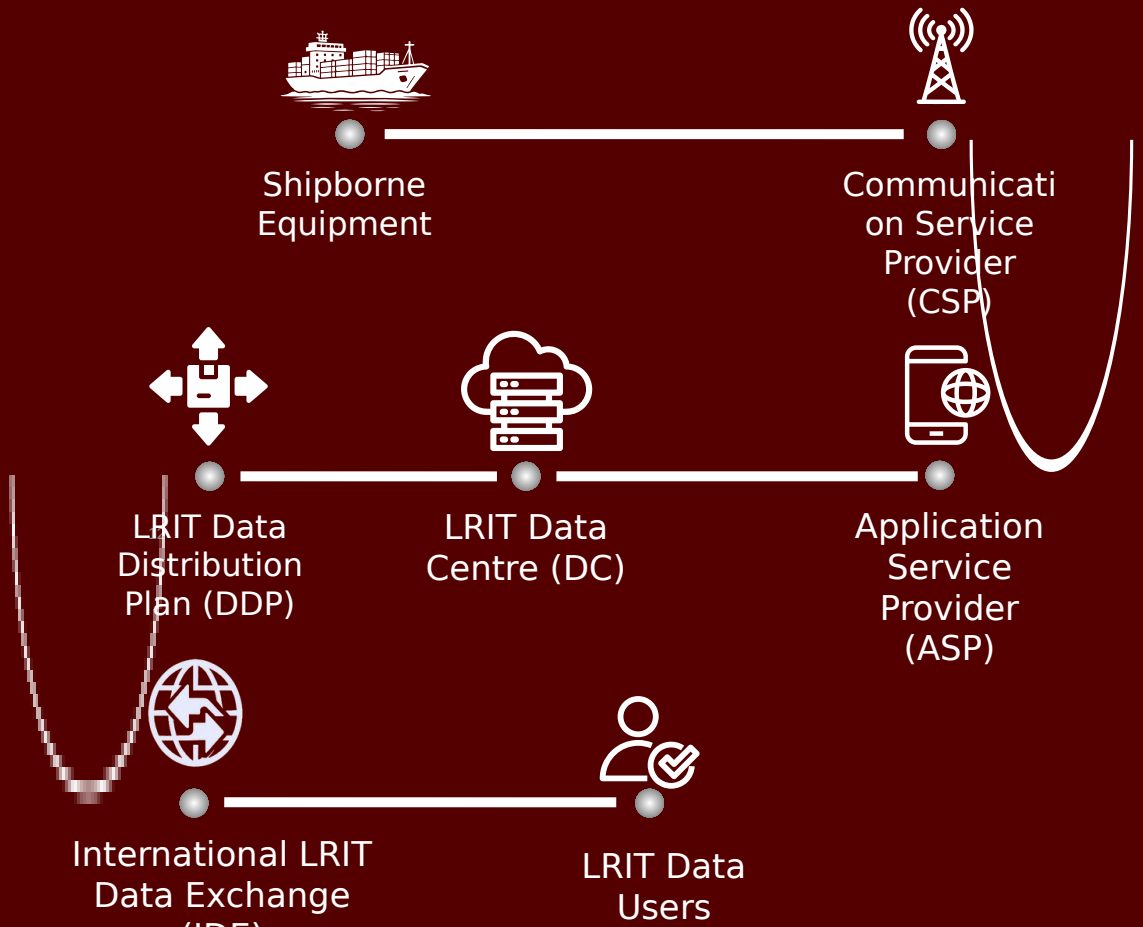


LRIT extends a nation's maritime vision beyond the coastline, enabling secure and intelligent oversight of global vessel movements.

- **Global Vessel Tracking**
- **Maritime Domain Awareness**
- **Security & Compliance**
- **Search & Rescue**

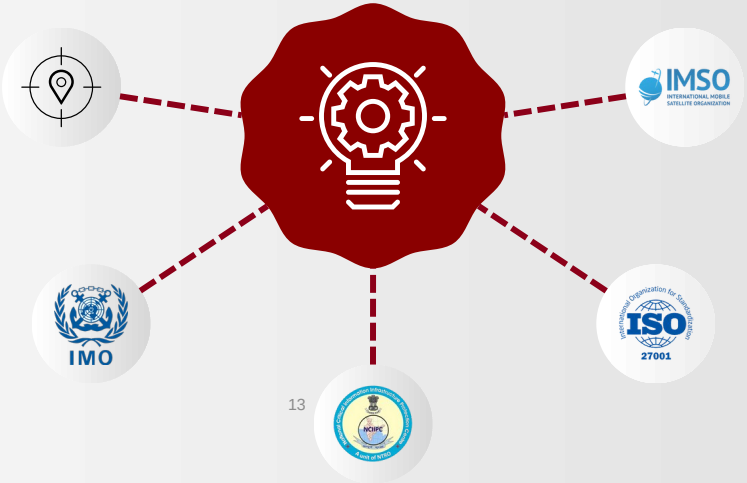
FUNCTIONS OF LRIT

- **The LRIT system transmits a vessel's identity, position, and timestamp via satellite from shipborne equipment.**
- **This data is routed through Communication and Application Service Providers to dedicated Data Centers.**
- **Distribution is controlled by a Data Distribution Plan, while global routing is handled by the International Data Exchange.**



PROMINENT FEATURES

Advanced GIS features for accurate incident analysis and Search & Rescue operations



Audited periodically by International Mobile Satellite Organization (IMSO)

Implemented in adherence to IMO standards and guidelines

National Data Centre and DRC set up as per NCIIPC and ISO 27001 guidelines

Designated as a "protected system" by the National Critical Information Infrastructure Protection Centre (NCIIPC)

Crypto in Daily Maritime Operations

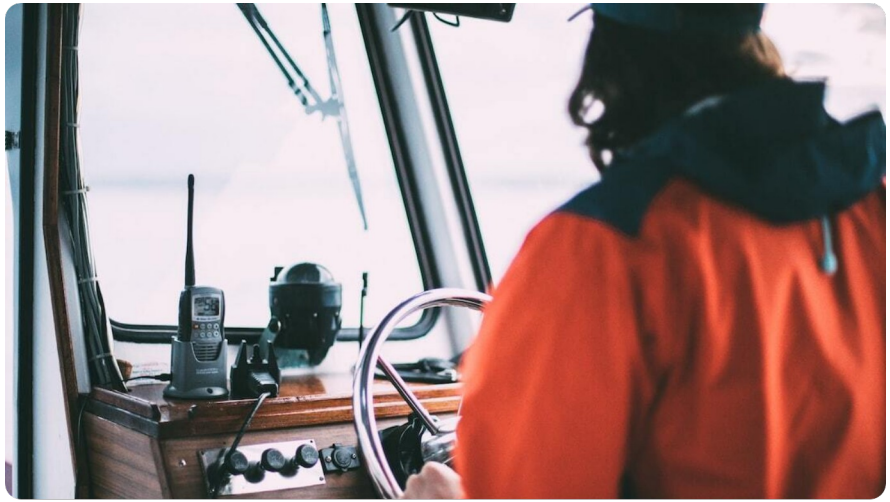
Digital Trust in Every Transaction

- **Digitally Signed Seafarer Credentials:** DG Shipping issues over 50,000 digitally signed certificates annually—including competency, medical fitness, and ratings documents—all verifiable globally.
- **Instant Authentication of Ship Certificates:** Safety, registration, and pollution prevention certificates carry cryptographic seals that enable real-time verification at any port worldwide.
- **Tamper-Evident Inspections:** Port and flag state control inspections now use e-signatures, ensuring integrity and auditability of reports and notices.
- **Trusted Training Credentials:** DG-approved training institutes issue digitally signed course completions and exam results, preventing fraud and ensuring compliance.

Digital Signatures in Practice

From the Bridge to the Bureau

- **Paperless Port State Inspections:** All port state control inspection reports and deficiency notices are now e-signed, enabling rapid processing and tamper-proof records.
- **Digital Flag State Survey Reports:** Flag state inspections generate digitally signed survey reports that maintain integrity from shipboard collection to regulatory submission.
- **Training Institutes and Fraud Prevention:** DG-approved institutes issue cryptographically signed course completions and exam results, drastically reducing credential fraud.
- **Device-Enabled Mobile Workflows:** Marine surveyors use tablets and smartphones to conduct inspections, capturing GPS/time-stamped, signed data across hulls, equipment, and operations.



Secure Survey and Port Processes

Data Integrity from Hull to Harbor

- **Digitized Ship Surveys:** Marine surveyors now use tablets to conduct cryptographically secured inspections with GPS/time-stamped digital reports.
- **Real-Time Data Authentication:** Each inspection record is digitally signed, ensuring tamper-evident transmission and end-to-end cryptographic security.
- **Integration with Classification Societies:** Statutory survey reports and certificates from classification societies are submitted digitally via secure portals to DG Shipping.
- **Streamlined Approvals and Audits:** Secure digital workflows reduce time lags in inspection approvals and facilitate transparent auditing of maritime safety processes.

Transformative Technologies

Cryptography, Blockchain & Maritime 4.0

Elliptic Curve Cryptography (ECC)
ECC powers secure, bandwidth-efficient digital bills of lading and shipboard communications, ideal for low-connectivity maritime environments.

Blockchain-Enabled Document Exchange
Platforms like CargoX digitize shipping documents with tamper-evidence and cross-border verifiability, enhancing transparency and trust.

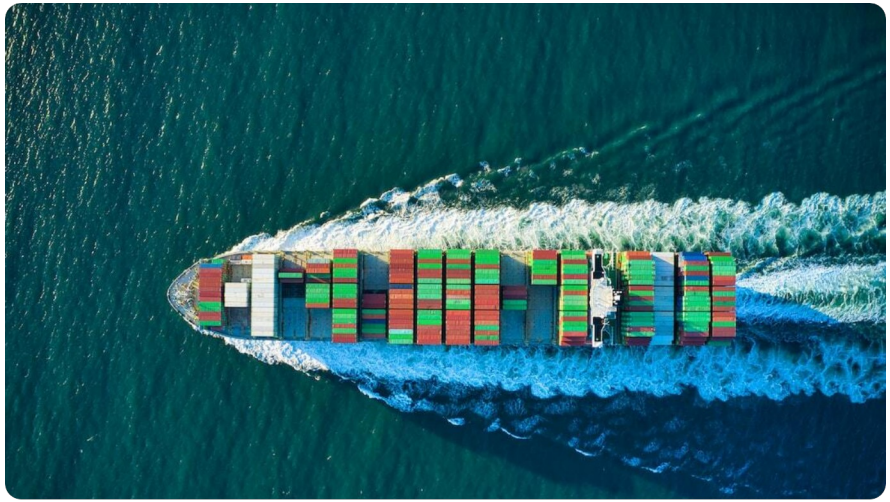
Smart Contracts for Port Automation
Digital contracts automate payments and delivery orders—triggered by real-time scans and integrated container tracking systems.

Marine Insurance Transformation
Digitally signed incident reports with cryptographic photo evidence expedite claims and reduce disputes in maritime insurance processes.

Standards & Regulatory Compliance

Building a Secure Maritime Ecosystem

- **IMO Cyber Risk Mandates:** DG Shipping aligns with IMO’s ISM Code amendments and Maritime Cyber Risk Management Guidelines to enforce onboard cyber resilience.
- **IACS Cyber Requirements:** Adherence to IACS UR E26 & E27 ensures cyber resilience in vessel design, essential for new ship approvals and certifications.
- **National Data Protection Law:** India’s Digital Personal Data Protection Act, 2023 governs seafarer identity and certificate issuance with encrypted personal data management.
- **From Compliance to Strategy:** Regulations are not mere checkboxes—they form the architectural foundation for security, accountability, and trust at scale.



Strengthening Cyber Resilience in Maritime Governance

Recognizing the increasing digitalization of maritime operations, DGS has initiated robust cybersecurity transformation. A unified cybersecurity compliance framework has been developed, aligning with global standards such as:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- ISO/IEC 27001 (Information Security)
- ISO 22301 (Business Continuity)
- ISO 31000 (Risk Management)
- European Union Agency for Cybersecurity (ENISA) Guidelines
- National regulations including Ministry of Electronics and Information Technology (MeitY), National Critical Information Infrastructure Protection Centre (NCIIPC), Standardisation Testing and Quality Certification Directorate (STQC) norms

This comprehensive approach aims to ensure end-to-end cybersecurity compliance for all digital and maritime systems, including port infrastructure and Vessel Traffic Management Systems (VTMS).

DGS Maritime Trust Framework

Scaling Digital Trust Across the Ecosystem

Universal Digital Signatures
Every maritime document—crew licenses, ship surveys, port clearances—will be digitally signed and globally verifiable.

Unified Signing Platform
A single e-signature ecosystem for shipping lines, agents, ports, and institutes to streamline approvals and ensure accountability.

Trust Through Audits & Drills
Routine cyber audits, incident response drills, and document verification protocols reinforce maritime cyber resilience.

Alignment with IMO & DPDP
The framework complies with IMO cyber guidance and India’s DPDP Act, integrating security into every layer of digital infrastructure.

Looking Ahead – Maritime Digital India 2030

A Vision for Secure, Seamless, Scalable Innovation

Universal Digital Identity
Every vessel and seafarer will have a unique, verifiable digital identity backed by cryptographic keys and role-based access.

End-to-End Encryption Ecosystem
Port-to-port document flows will be encrypted and traceable—covering clearances, training, contracts, and communications.

Controlled Innovation Sandboxes
Blockchain pilots, smart contracts, and digital currency use cases will be tested in maritime sandboxes with regulatory oversight.

Global Interoperability by Design
Systems will comply with international maritime cybersecurity protocols, enabling cross-border trust and seamless verifications.

Closing & Call for Collaboration

Trust as a Compass for the Maritime Future

Cryptography as the Foundation
From distress alerts to cargo manifests, digital trust is the bedrock of modern maritime operations.

Digital Signatures: Enablers of Scale
E-signatures enable secure, auditable, and instant approvals—at scale, across borders, and with legal validity.

Collaboration is Non-Negotiable
Progress demands joint effort: regulators, academia, startups, and industry must co-create scalable trust architectures.

Call to Action
Let us join to developing secure enclaves, spoofing detection, PKI frameworks, and cross-border verifications.

Thank You