CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Maritime Criminality and Cybersecurity: Strengthening Global Regulatory Responses

Dr. Su Wai Mon

Research Fellow (Ocean Law & Policy)

Centre for International Law

National University of Singapore

su.wm@nus.edu.sg

Maritime Security Threats

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Category	Threats	Relevant Legal Framework
Traditional Security Threats	Naval warfare, armed conflict, inter-state military confrontation	International Humanitarian Law (IHL), Law of Naval Warfare
Non-Traditional Security Threats	Piracy and armed robbery, maritime terrorism, IUU fishing, trafficking and smuggling, marine pollution, **maritime cybersecurity, protection of critical maritime infrastructure**	United Nations Convention on the Law of the Sea (UNCLOS 1982), International Maritime Organization (IMO) Conventions, Regional cooperation mechanisms, National legislation

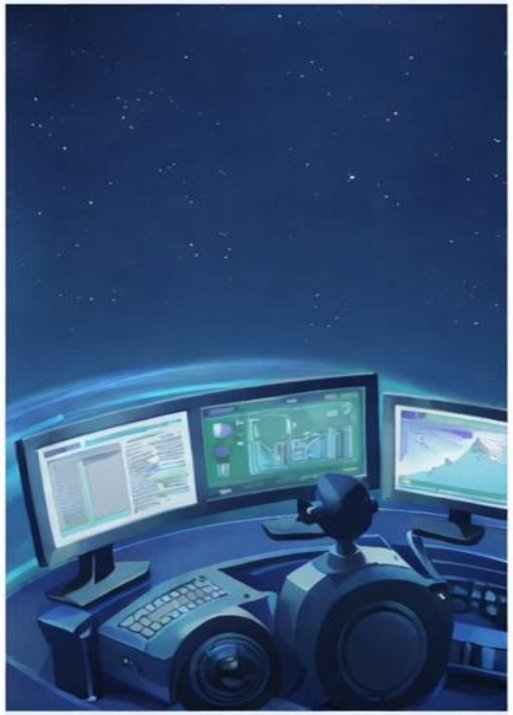
Domains Relevant to Maritime Security

Land

Sea

Undersea

Cyber/Digital



Space

RSIS COMMENTARY

27 February 2026

Protecting Critical Maritime Infrastructure: A Multi-Domain Approach to Maritime Security Governance

Su Wai Mon

CIL
OR INTERNATIONAL LAW
Jniversity of Singapore

“

In the real world, cyber is not just zeros and ones and bytes and bits. It’s operational technology that changes the physical world, and that makes it dangerous.

MICHAEL THOMPSON


PREVENTION
Better than Cure
CURE
Prevention is Better than Cure

IT–OT Integration in the Maritime Industry

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- **Previously:** IT and OT systems operated separately from each other and from on-land networks.

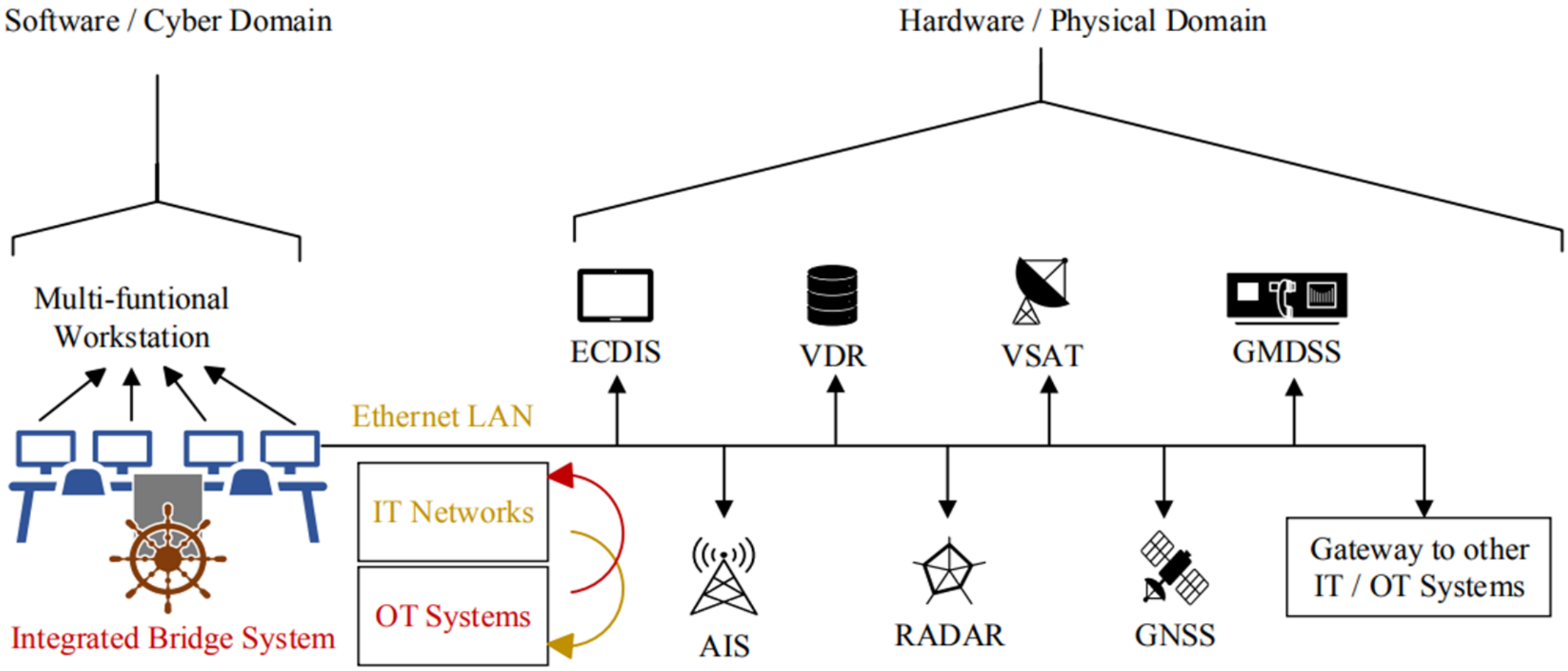
- **Now:** Digitalisation has led to growing interconnection between IT and OT systems in the maritime industry.

- **Maritime transport involves:**
  - ✓ Shore-based IT/OT – technologies for port and logistics operations.
  - ✓ Seaborne IT/OT – systems managing ship operations.

- **Operational Technology (OT):** Controls engines, cargo management, navigation, and administrative functions.

- **Challenge:** Maritime OT is less advanced and more vulnerable to cyberattacks, posing safety risks to ships and crews.

Ship IT and OT systems



MARITIME CYBERSECURITY

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Maritime Infrastructure	Key Threats	Why it matters to protect them
Ships	GPS spoofing, ransomware, remote hijacking	• Ensures safe navigation and route integrity • Prevents unauthorized control of critical systems • Protects crew, cargo, and environment
Ports	Terminal system hacks, data breaches, access control failures	• Maintains cargo flow and global trade stability • Secures supply chains and customs data • Prevents economic disruption and smuggling
Offshore Facilities	ICS/SCADA attacks, remote shutdowns, cyberattacks targeting industrial control systems that can lead to physical damage, operational disruption, and safety risks	• Protects energy infrastructure (oil, gas, wind) • Prevents environmental and safety incidents • Ensures production continuity

SYSTEM DOWNTIME in Critical Infrastructure

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- Leads to significant **economic loss**
- Causes **damage to the corporate reputation**
- Poses a **serious risk to human lives**

Global Impact: Cybercrime is projected to cost over **USD 10 trillion worldwide by 2025** (Britannia P&I Club).

Maritime Impact: While shipping accounts for a small share, each cyberattack in the maritime sector costs organisations **an average of USD 550,000.**

RISKS: NATIONAL SECURITY, ECONOMY, ENVIRONMENT

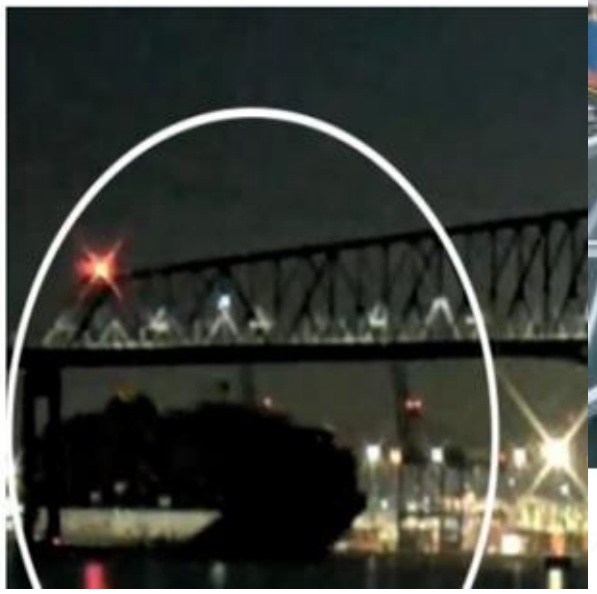
CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- **National Security:** Security of Critical National Infrastructures
- **Environment:** Damage to the marine environment
- **Economy:** Worldwide economic losses (If 15 Asian ports were hacked, financial losses would be more than US$110 billion. (Lloyd's report)

CRISIS SCENARIOS

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Ship that struck Baltimore bridge lost power twice before crash, NTSB preliminary report finds



Reuters

Six workers presumed dead after crippled cargo ship knocks down Baltimore bridge | Reuters

A SATELLITE PHOTOGRAPH REVEALS HOW THE EVER-GIVEN WAS WEDGED ACROSS THE CANAL (SOURCE :BBC NEWS)

2021 Suez Canal obstruction

BP Oil Spill Environmental Impact

Security

US offshore oil and gas rigs at 'significant' risk of cyberattacks, warns government watchdog

Carly Page / 7:01 AM PST • November 22, 2022

Singapore

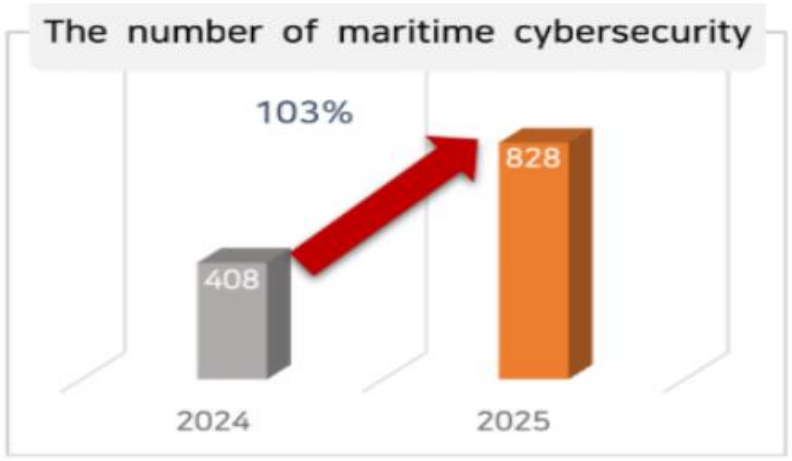
CNA Explains: What we know about the Singapore oil spill that's affected Sentosa and other beaches

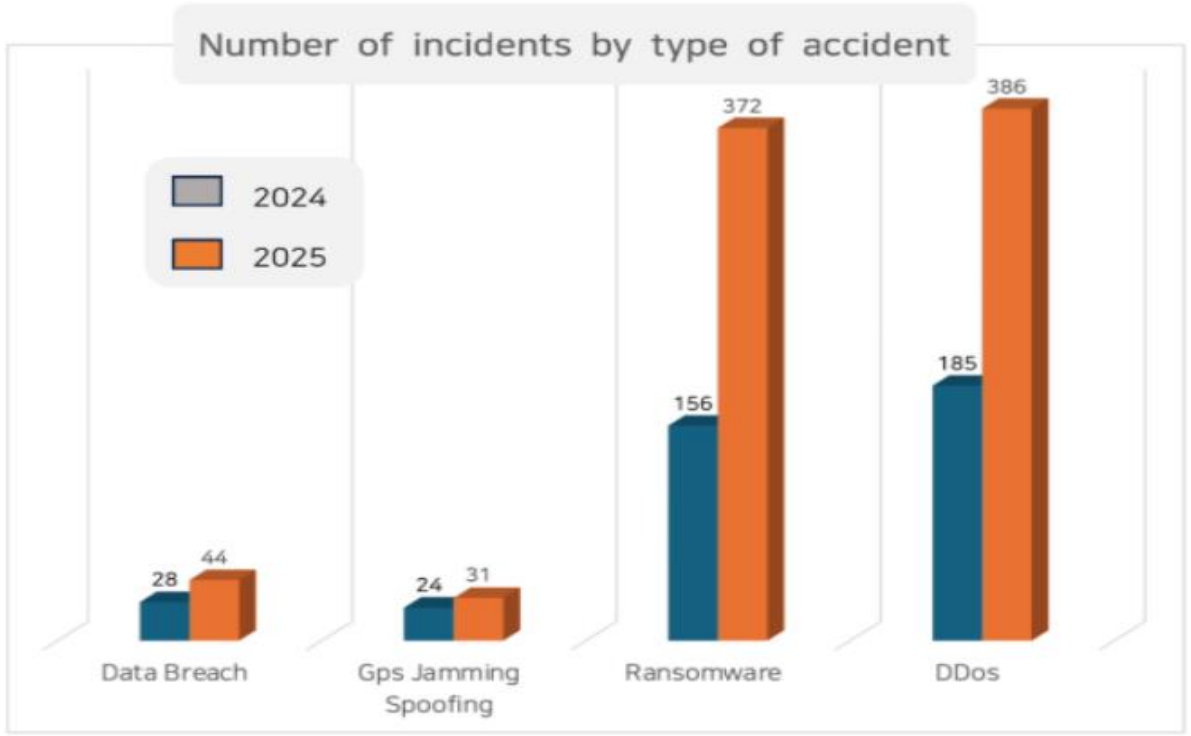
CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

About 400 tonnes of fuel were released into the sea on Friday. An accident over two decades ago involved 7,000 tonnes - but that wasn't Singapore's largest oil spill ever.

Justin Ong Guang-Xi

19 Jun 2024 06:00AM
(Updated: 04 Feb 2026 03:13PM)





CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

According to the ***CYTUR report,*** compared to 2024, the number of maritime cyber incidents in 2025 surged by 103%, emerging as a critical threat to maritime safety.

REPORTED INCIDENTS

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Jonathan Greig
January 17th, 2023

Malware | Briefs | Cybercrime

Ransomware attack on maritime software impacts 1,000 ships

About 1,000 vessels have been affected by a ransomware attack against a major software supplier for ships.

Oslo-based DNV – one of the world's largest maritime organizations – said it was hit with ransomware on the evening of January 7 and was forced to shut down the IT servers connected to their ShipManager system.

"DNV is communicating daily with all 70 affected customers to update them on findings of the ongoing forensic investigations. In total around 1000 vessels are affected," DNV said in a statement on Monday.

"All users can still use the onboard, offline functionalities of the ShipManager software. There are no indications that any other software or data by DNV is affected. The server outage does not impact any other DNV services."

LAB DOOKHTEGAN CYBER ATTACK ON IRANIAN OIL TANKERS DISRUPTS OPERATIONS

The Iranian anti-government hacktivist group "Lab Dookhtegan" ("sealed lips" in Farsi) announced on March 18th, 2025, that it had successfully disrupted all communications for 116 oil tanker ships belonging to two Iranian companies that are associated with the government and allegedly operate against international sanctions. The group claims that the attack prevented communications both on the ship and ship-to-shore (Satcom).

Communication devices are the bottleneck of maritime vessels. While modern communications devices can connect to multiple satellite (and terrestrial, e.g., 4/5G) connectivity services for redundancy, few are designed for cyber resilience, and in many cases, cyber protection is even embedded within the communications devices. This makes the ship's communication device a single point of failure, and if a malicious actor hacks the communication device (VSAT or other), it can take complete control over all communications of the vessel and even spread out to the IT and OT systems.

CY

YOU ARE INVI

CIL

FOR INTERNATIONAL LAW

l University of Singapore

Lab Dookhtegan hacking group allegedly disrupted communications of 60 Iranian ships run by sanctioned firms NITC and IRISL.

The hacking group Lab Dookhtegan allegedly disrupted the communications of 60 Iranian ships. The attack hit at least 39 tankers and 25 cargo ships operated by Iranian maritime companies National Iranian Oil Tanker Company and Iran Shipping Lines, which the US sanctioned.

Hackers breached the satellite communications company Fannava, disabling the Falcon communications system and wiping core data. The attack left the Iranian ships blind.

The group published screenshots demonstrating they achieved root access on Linux terminals running iDirect satellite software (version 2.6.35). The software is considered ancient and not compliant with basic cybersecurity standards.

TECHNOLOGY

Japan's biggest port, Nagoya, hit by suspected cyberattack

Ransomware shuts down Toyota's export hub

CIL

CENTRE FOR INTERNATIONAL LAW

apore

PORT TECHNOLOGY INTERNATIONAL

Home About News Journal Technical Papers Events Webinars Supplier Direct

Safety and Security, People, Ports and Terminals

DP World Australia hit by cyber attack

November 30, 2023

By Dom Magli

TWITTER FACEBOOK LINKEDIN EMAIL

Cyber attack hits state-owned terminal at India's JNPT

February 22, 2022

Facebook Twitter Linkedin Email

Insider Threats

GTMARITIME Products Solutions Support Insights Company

The Growing Risk of Insider and Physical Attacks

Insider threats and physical access are becoming increasingly important in maritime cyber risk.

The NORMA assessment notes that threat actors are likely to exploit access through crew, contractors, or maintenance personnel to introduce malicious hardware.

Combined with the low cost and accessibility of devices like Raspberry Pi, this creates a scalable and difficult-to-detect method of attack.

In short, cyber threats in the maritime industry are no longer purely digital – they are physical, operational, and hybrid.

amazon.sg Delivering to Singapore 350000 Update location All Search Amazon.sg EN Hello, sign in Account and Lists

All Fresh & Fast Best Sellers Today's Deals Prime Books Electronics Home Computers Pet Supplies

Sign in New customer? Start here.

Electronics Mobile Phones & Accessories Headphones Speakers TV & Video Cameras Tablets Wearable Technology Batteries & Chargers

Electronics › Computers, Components and Accessories › Components & Replacement Parts › Internal Components › Motherboards

Click to see full view

Raspberry Pi 5 4gb

Brand: Raspberry Pi

4.7 ★★★★☆ (1,482)

Amazon's Choice

S$183.60

Sign in to redeem. Buy 2, save 10% promo code: UZEMCGEECRLD Shop items ›

Sign in to redeem. Prime Savings Save 5% promo code: MDJMSKJNEHHG Shop items ›

Prime Savings Buy 2, save 10% Shop items ›

Secure transaction Returns Policy

Size Name: 4 GB

S$183.60

FREE deliver Details

Or fastest de May. Details

Delivering Update loc

In stock

US imports r local produc

apply. Learn

Quantity:


Low Awareness
Lack of National legislation
Attribution
Existing Challenges for Ship Cybersecurity
Lack of Standardized Technical Frameworks for Cyber
Fragmented Regulatory Framework for Ships and Other Maritime Systems and Infrastructure

Prevention

- Compliance

- Compliance
- Cooperation and Coordination

Cure

National Legislation Criminalising Cyber Attack against Critical Maritime Infrastructure including Ships.

For this purpose attribution is a major challenge

Maritime Cybersecurity Governance

Prevention	Cure
Cybersecurity (cyber resilience of critical maritime infrastructure) Proactive	**Cybercrime** (criminalising cyber attacks against critical maritime infrastructure) Reactive Budapest Convention 2001; UN Convention Against Cyber Crime 2025
Needs **standards, regulation, compliance (IMO, flag/port state controls), risk management**	Needs **criminal law, attribution, prosecution, international cooperation**

Existing Framework	Scope
IMO Resolution MSC.428(98)- entered into force on 1st January 2021	- To incorporate cyber risk management into their safety management system (ISM) Code under the SOLAS.
IMO Maritime Cyber Risk Management Guidelines MSC-FAL.1/Circ.3 Rev 3 , April 2025	-Non-binding guidelines which outline key functional elements for cyber risk management : *Identify, Protect, Detect, Respond and Recover.*
The International Association of Classification Societies (IACS) Unified Requirements: UR E26 and UR E27	-Binding requirements to strengthen maritime cybersecurity by incorporating cyber resilience into ship design and control system. UR E26 (cybersecurity by design) and UR E27 (OEM)
ISPS Code under SOLAS	-adopted to enhance security and prevent incidents affecting ships and port facility (ship-port interface)
Standards and Best Practices for Implementation of Cyber Risk Management	-ISO/IEC 27001 on information technology -Guidelines on Cybersecurity on board ships adopted by the industry including BIMCO, INTERTANKO

SUA Convention and 2005 Protocols

Convention	Purpose	What it covers:
The Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention),	The objective of the Convention is to criminalize unlawful acts against ships and ensure that offenders are either prosecuted or extradited.	• the seizure of ships by force; • acts of violence against persons on board ships; and • the placing of devices on board a ship which are likely to destroy or damage it.
Protocol for the Suppression of Unlawful Acts Against the Safety of **Fixed Platforms Located on the Continental Shelf (1988)**	Extends the SUA Convention to **fixed platforms** (e.g., offshore oil rigs, gas platforms)	• Attacks against offshore installations • Seizure of platforms • Violence against persons on platforms • Destruction or damage to platforms
2005 SUA Protocols (Amendments to 1988 Instruments)	To address **modern maritime security threats**, especially after **9/11** and growing terrorism concerns. New powers: • **Ship boarding provisions.** • States can **request boarding of suspect ships** on the high seas	➢ **2005 SUA Protocol,** amending the **1988 SUA Convention** • ***Adds:*** Maritime terrorism WMD transport Ships used as weapons ➢ **2005 Fixed Platforms Protocol** • Amends the **1988 Fixed Platforms Protocol** • ***New threats added*** • WMD and terrorism • emerging threats

Key Developments in IMO Maritime Cybersecurity and Digitalization

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- **International Maritime Organization Digitalization Strategy Approved (March 2026)**

The IMO Facilitation Committee (FAL Committee) approved the IMO Strategy on Maritime Digitalization to enhance interoperability, system standardization, data-sharing, and effective data governance across maritime stakeholders.

- **Mandatory Cybersecurity for Maritime Single Windows**

The FAL Committee approved amendments to the Annex of the to the Convention on Facilitation of International Maritime Traffic (FAL Convention) 1965 requiring Contracting Governments to **implement mandatory cybersecurity measures** to protect maritime single windows in line with national legislation.

- **Development of Maritime Cyber Code (by 2028)**

The IMO Maritime Cyber Code is under development as a non-mandatory, flexible framework covering ships, ports, and ship-shore interfaces, adaptable to national and regional requirements.

Relevant IMO Conventions

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- The International Convention for the Safety of Life at Sea (SOLAS) 1974
- Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs)
- International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978
- Facilitation of International Maritime Traffic (FAL Convention) 1965

Recommendations & Way Forward

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- Strengthening Flag State Implementation of the ISM Code
- Strengthening Port State Control Inspections
- Implementing IACS Cybersecurity Requirements
- Integrating cybersecurity requirements for ISPS Code Implementation
- Strengthening Domestic Cybersecurity Legal Frameworks
- Ratification of the UN Convention on Cybercrime
- Development of IMO Cyber Code (Technical aspect)
- Designating point of contact
- Information-sharing
- Inter-agency cooperation
- Regional and International cooperation

FUTURE: The IMO has determined four degrees of Maritime Autonomous Ships

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

1. **Degree one:** Ship with automated processes and decision support. *Seafarers are on board* to operate and control shipboard systems and functions;
2. **Degree two:** Remotely controlled ship *with seafarers on board.*
3. **Degree three:** Remotely controlled ship *without seafarers on board.*
4. **Degree four:** *Fully autonomous ship*. The operating system making decision on its own

The mandatory MASS Code is intended to be adopted by 1 July 2030, with entry into force from 1 January 2032

BRILL
NIJHOFF

ASIA-PACIFIC JOURNAL OF OCEAN LAW AND POLICY
8 (2023) 329–351

APOC
brill.com/apoc

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Improving Maritime Cybersecurity in Southeast Asia: Suggestions for Further Action by ASEAN

Vu Hai Dang
Researcher, Diplomatic Academy of Viet Nam, Hanoi, Vietnam
haidangvu@gmail.com

Su Wai Mon
Senior Lecturer, Faculty of Law, University of Malaya, Kuala Lumpur, Malaysia
suwai.mon@um.edu.my

Received: 7 August 2023 | Accepted: 15 August 2023 |
Published online: 15 December 2023

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore