

CYBER THREATS IN THE MARITIME DOMAIN: AN EMERGING MARITIME SECURITY CHALLENGE

Dr. Su Wai Mon

Research Fellow (Ocean Law & Policy)

Centre for International Law

National University of Singapore

su.wm@nus.edu.sg

CYBERSECURITY OF MARITIME INFRASTRUCTURES

CIL

CENTRE FOR INTERNATIONAL LAW
National University 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

IT–OT Integration in the Maritime Industry

- **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.

MARITIME CYBERSECURITY



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, sabotage 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

- 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.**

Colonial Pipeline begins restart efforts after disruptive cyberattack in U.S.

Ransomware attack on Colonial Pipeline last week halted shipment of 2.5 million barrels per day

Thomson Reuters ·

Posted: May 12, 2021 7:18 AM MST | Last Updated: May 13, 2021



RISKS: NATIONAL SECURITY, ECONOMY, ENVIRONMENT

- **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

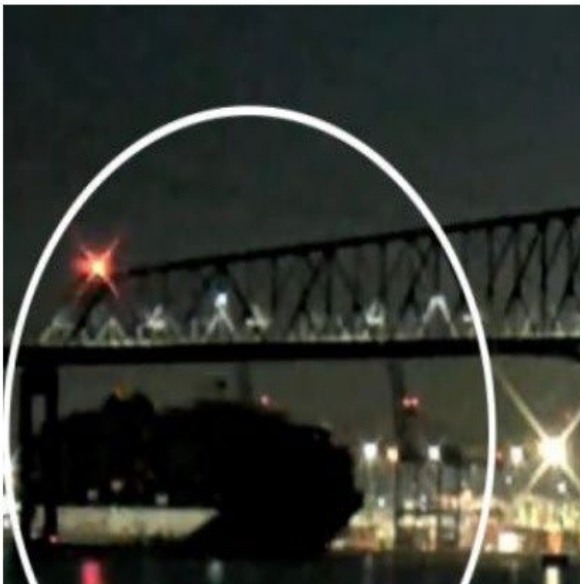


By Pete Muntean, Gregory Wallace and Eric Le

4 minute read · Updated 5:15 PM EDT, Tue



Reuters

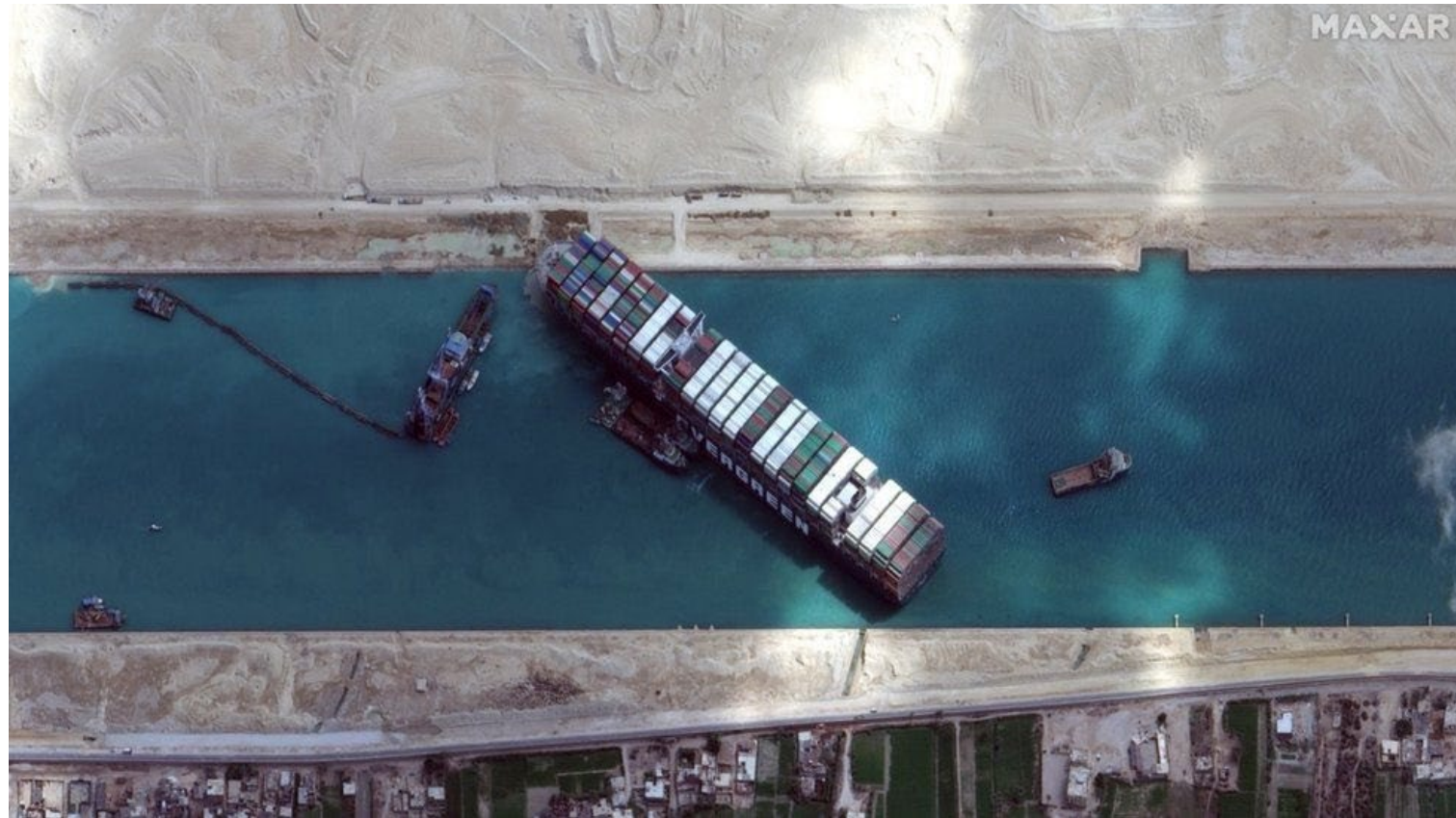


Six workers presumed dead after crippled cargo ship knocks down Baltimore bridge | Reuters

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

CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore



20 APRIL 2010 – LARGEST MARINE OIL SPILL IN THE HISTORY OF PETROLEUM INDUSTRY

CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

BP Oil Spill Environmental Impact



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

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



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."

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

Ransomware shuts down Toyota's export hub

[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](#)

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.

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.



CY

VOII ADE INVIT

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

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

EXISTING REGULATORY FRAMEWORKS ON MARITIME CYBERSECURITY

IMO Resolutions & Maritime Cyber Risk Management Guidelines MSC-FAL.1/Circ.3/Rev.3 (Revised April 2025)

Additional Standards:

- IACS Unified Requirements UR E26/27 (effective 1 July 2024)
- ISO/ICE 27001 standard on Information Technology-security techniques-Information security management systems-Requirements.

International Guidelines and Industry Best Practices recognized by IMO

- *Consolidated IACS Recommendation on cyber resilience (Rec 166).*
- *The Guidelines on Cybersecurity Onboard Ships, produced and supported by ICS, INTERTANKO, INTERCARGO, IUMI, BIMCO, OCIMF, Intermanager, WSC and SYBAss.*
- *Cybersecurity Guidelines for Ports and Port Facilities by the International Association of Ports and Harbors (IAPH) 2021 & 2025*
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST 2.0 Framework)
- IAPH Cybersecurity Guidelines for Ports and Port Facilities.

CHALLENGES In addressing Maritime Cybersecurity

- Low level of awareness regarding cyber threats across the sector
- Underreporting of cyber incidents
- Limited investment in cybersecurity infrastructure and workforce
- Absence of national maritime cybersecurity policies and legislation
- Shortage of skilled personnel and enforcement capacity
- Reactive posture — need for proactive strategies
- Lack of cyber resilience across key functions:
Identify, Protect, Detect, Respond, Recover

RECOMMENDATION for Coordination and Collaboration

	Cooperative Actions
State Level	• Identify Maritime Critical Infrastructures • Develop a Comprehensive National Maritime Security/Cybersecurity Policy • Legal framework
Regional Level	• Enhance Regional Collaboration & Information Sharing and joint maritime cybersecurity drills • Promote Harmonized Regulatory Standards
International level	• Strengthen Global Governance • Engage with IMO, Industry Bodies & Maritime Cybersecurity Alliances

WAY FORWARD

- **Balance Economic Interests with Security Priorities**
Ensure cybersecurity is treated as a strategic enabler, not a cost burden.
- **Adopt a Proactive, Forward-Looking Approach**
Shift from reactive responses to anticipating and mitigating future threats.
- **Foster Public–Private Cooperation**
Enhance collaboration between governments, industry, academia, and think tanks.
- **Invest in Capacity Building**
Strengthen technical expertise, awareness, and training across the maritime workforce.
- **Promote Information Sharing**
Establish trusted platforms for reporting incidents and exchanging threat intelligence.
- **Move Toward Holistic and Unified Governance**
Develop an internationally coordinated regulatory framework to standardize practices and close security gaps.

Publications



BRILL

[Browse Our Titles](#)

[Subjects](#)

[Authors](#)

Strengthening Australia-ASEAN Cooperation in Maritime Cybersecurity

PUBLISHED 12 MAR 2024



SU WAI MON

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

In: [Asia-Pacific Journal of Ocean Law and Policy](#)

Authors: [Vu Hai Dang](#) and [Su Wai Mon](#)

Online Publication Date: 15 Dec 2023

[Abstract](#) [Full Text](#) [PDF](#) [Metadata](#) [Metrics](#)

[OPINION] Malaysia needs to be proactive in dealing w emerging cyber threats in the maritime domain

AWANI
INTERNATIONAL

AWANI Columnist

29/04/2024 | 10:00 MYT



Editor's Note: The 2024 ASEAN-Australia Special Summit Maritime Cooperation Forum was held last week in Melbourne. This article is part of the 'Blue Security' project led by La Trobe Asia, University of Western Australia Defence and Security Institute, Griffith Asia Institute, United States Studies Centre, UNSW Canberra and the Asia-Pacific Development, Diplomacy and Defence Dialogue (AP4D). Views expressed are solely of its author/s and not representative of the Maritime Exchange, the Australian Government, or the collaboration partner country government.

THANK YOU FOR YOUR KIND
ATTENTION