CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

MARITIME CYBERSECURITY: ADDRESSING REGULATORY CHALLENGES AND THE IMPERATIVE FOR INTERNATIONAL COLLABORATION

Dr. Su Wai Mon

Research Fellow

Centre for International Law

National University of Singapore

5th Maritime Security Conference, 24-25 June 2025,
MARSEC COE, Istanbul, Turkey

CYBERSECURITY OF MARITIME INFRASTRUCTURES

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore




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 (Industrial Control Systems/Supervisory Control and Data Acquisition Systems)attacks, remote shutdowns, sabotage	• Protects energy infrastructure (oil, gas, wind) • Prevents environmental and safety incidents • Ensures production continuity

Key questions:

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

WHO : Threat actors

WHY : attack?

WHAT: Impacts/Risk/ Challenges

HOW : Risk management/ Mitigation

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**

- According to Britannia P&I Club, global costs from cybercrime predicted to exceed **USD 10 trillion by 2025.**
- Although shipping contributes a small part of this total, cyber attacks in the maritime industry now cost the targeted organisation 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

- Fuel Shortages & panic buying
- Stations ran out of fuel
- Fuel prices rose to highest point since 2014

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

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)

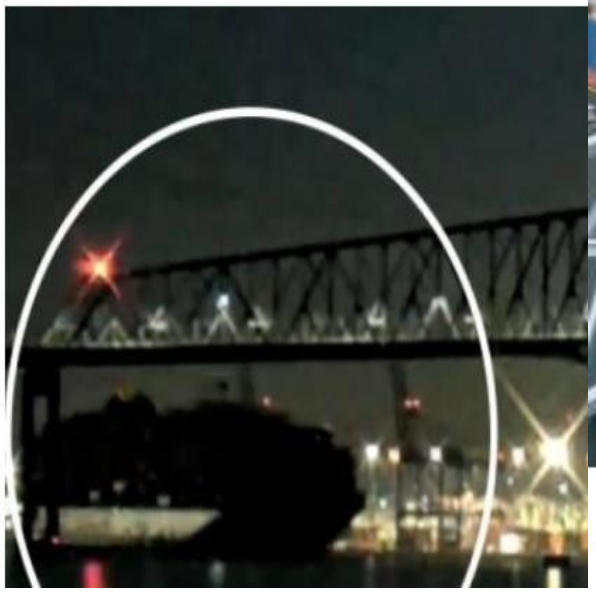
CRISIS SCENARIOS

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

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

By Pete Muntean, Gregory Wallace and Eric Le

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

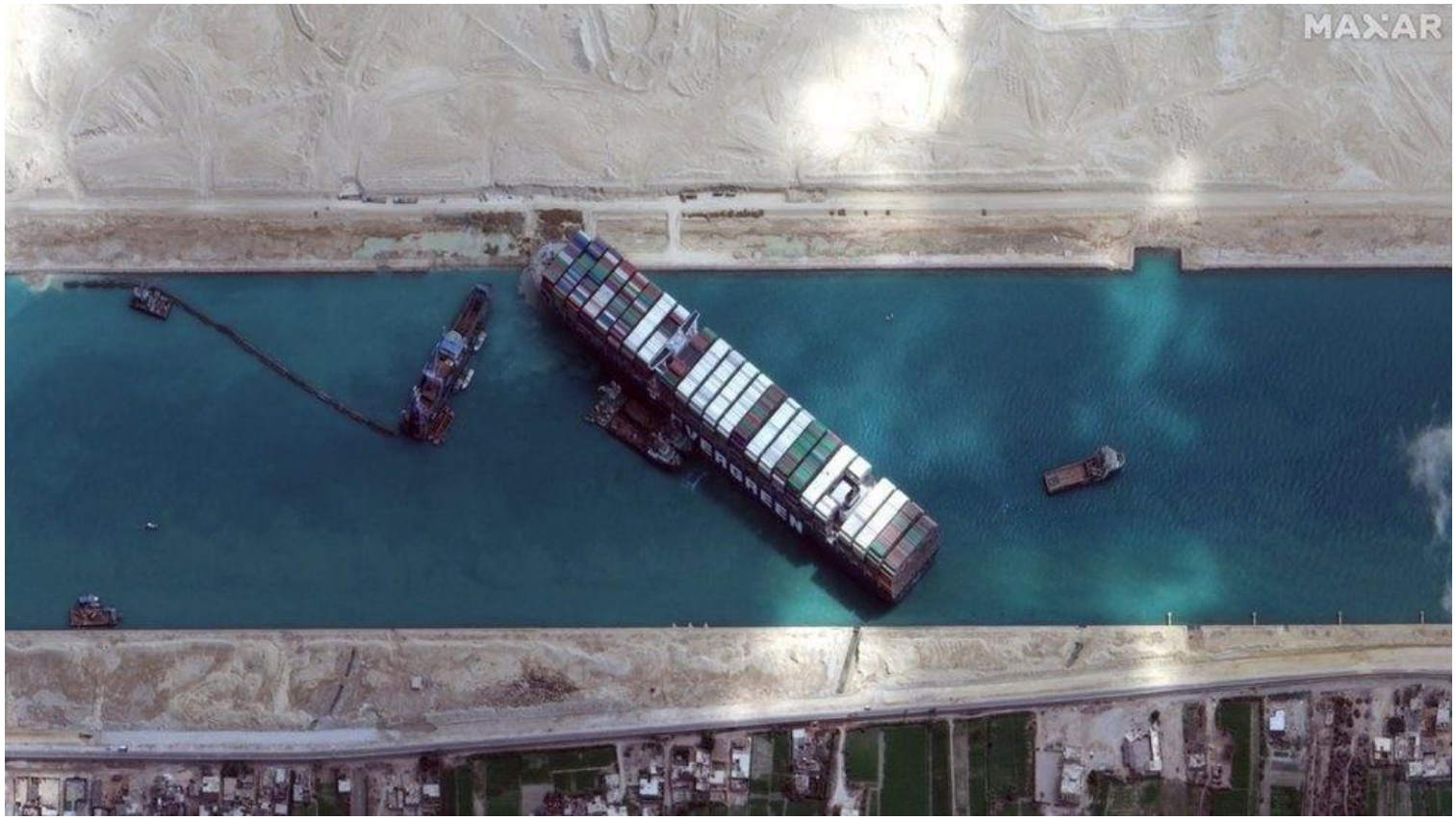


Reuters

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

Security

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

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

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

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."

TECHNOLOGY

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

Ransomware shuts down Toyota's export hub

PORT TECHNOLOGY INTERNATIONAL

CIL

Home About News Journal Technical Papers Events Webinars Supplier Directo

2023 Ransomware

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

SAFETY4SEA

Safety | SEAFiT | Green | Smart | Risk | Others | Columns | Events | Plus

Hackers claim to have disrupted communications to Iranian ships

by The Editorial Team — March 21, 2025 in Cyber Security

The hacke
responsib
networks

March 2025

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Digital Ship

NEWS | BIG READS | DOWNLOAD MAGAZINE | EVENTS | ADVERTISE | VESSEL PERFORMANCE | CONTACT

Cydome: anti-Iran group claims to have hacked satcom terminals of 100 Iranian tankers by gaining login credentials

Thursday, March 20, 2025 Communications & Cyber Security

The Iranian anti-government hacktivist group "Lab Dookhtegan" ("sealed lips" in Farsi) announced yesterday that it has successfully disrupted all communications for more than 100 oil tanker ships belonging to two Iranian companies associated with the government and allegedly operating against international sanctions. The group claims that the attack prevented communications both on the ship and ship-to-shore (Satcom).

EXISTING REGULATORY FRAMEWORKS ON MARITIME CYBERSECURITY

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

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)
- 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

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- Low awareness of 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: **GOVERN,** Identify, Protect, Detect, Respond, Recover (NIST Framework)

RECOMMENDATION for Coordination and Collaboration

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

	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

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- **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.

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

THANK YOU