CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

MARITIME CYBERSECURITY: ADVANCING STRONER REGIONAL COOPERATION

Dr. Su Wai Mon

Research Fellow (Ocean Law & Policy)

Centre for International Law

National University of Singapore

su.wm@nus.edu.sg

Key Discussion Points

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

1. Maritime Cybersecurity and vulnerable maritime infrastructure?

2. Impact of Maritime Cyber Risks

3. Towards stronger Regional Cooperation

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 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

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

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.**

Who and Why?

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

Threat Actors	Motivation
Cyber Criminals	Financial Gain (ransomware, data theft/fraud, cargo theft. Smuggling)
Nation State Actors	Espionage and Information Gathering/Geopolitical Advantage/Cyber Warfare
Hacktivists	Espionage and Information Gathering
Cyber Terrorist	Ideological Beliefs/Thrill-Seeking

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)

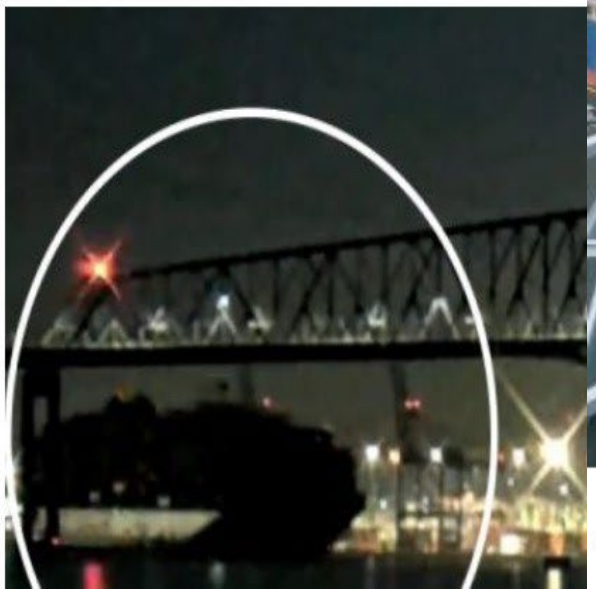
CRISIS SCENARIOS

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

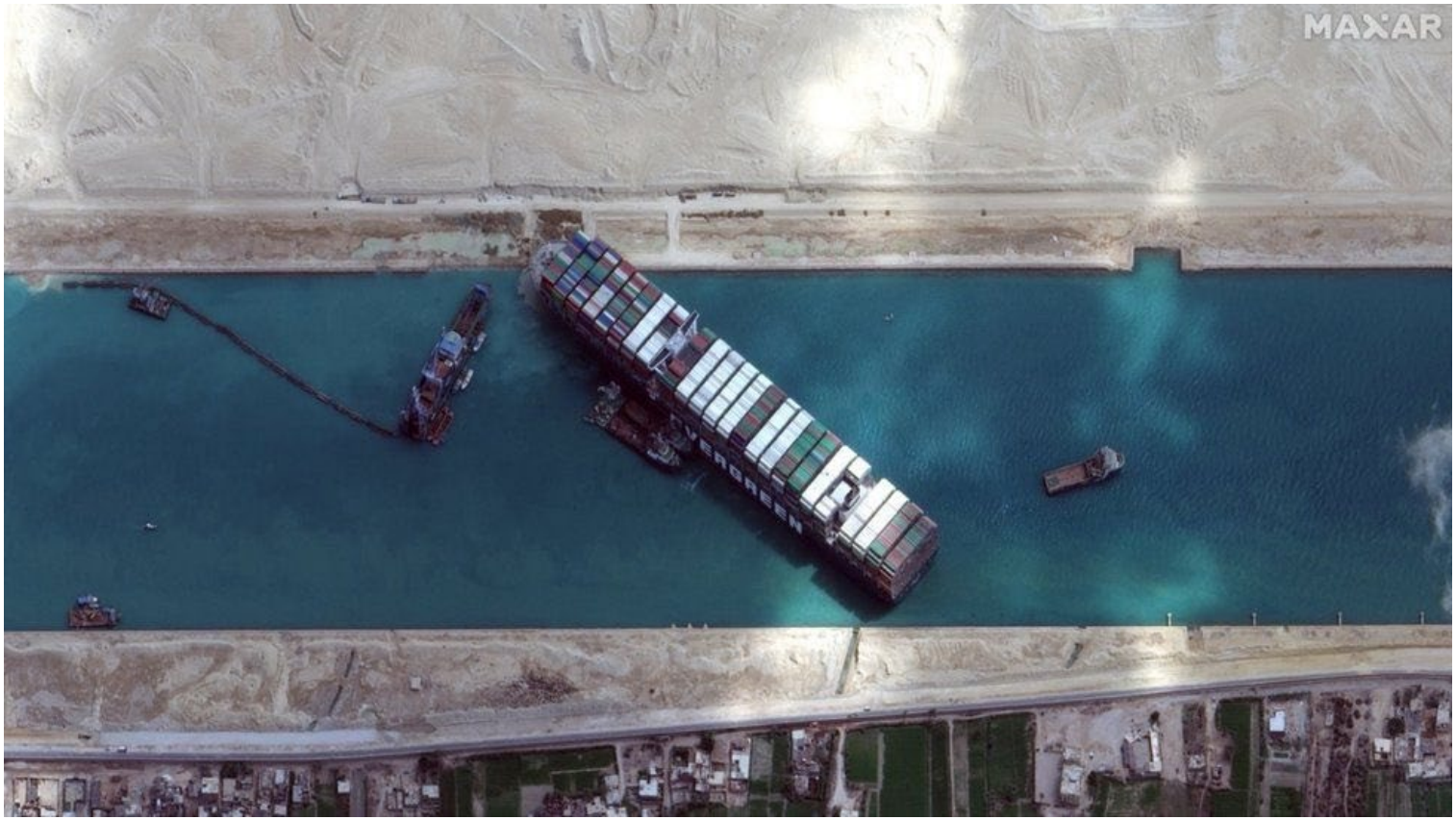


Reuters

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

DNV Norway Ransomware Attack

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

CIL

CENTRE FOR INTERNATIONAL LAW

PORT TECHNOLOGY INTERNATIONAL

Home About News Journal Technical Papers Events Webinars Supplier Directo

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.

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

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) 2021 & 2025
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST 2.0 Framework)

CHALLENGES In addressing Maritime Cybersecurity

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- 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
- Need to strengthen cyber resilience across key functions: **Identify, Protect, Detect, Respond, Recover**

Best Practices: National & Regional Approaches

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- **US Coast Guard:** the final rule effective date, **July 16, 2025,** targeted at *U.S.-flagged vessels, Outer Continental Shelf (OCS) facilities, and facilities subject to the Maritime Transportation Security Act of 2002 (MTSA);* All reportable cyber incidents must be reported to the National Response Center

- UK Cybersecurity Code of Practice for Ships (COP); first issued in 2017 and updated in 2023

- The Network and Information Systems Directive 2 (Directive 2022/2555, also known as **NIS2**) establishes a **unified legal framework to uphold cybersecurity in 18 critical sectors across the EU** and calls on Member States to define national cybersecurity strategies and collaborate with the EU for cross-border reaction and enforcement. **(transport, energy, finance and digital infrastructure**).

The Maritime Testbed of Shipboard Operational Technology (MariOT) system was commissioned by the Maritime Port Authority in partnership with SUTD Centre for Research in Cyber Security, iTrust and industry partners.

Maritime Cyber Attack Database (MCAD)

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

NHL STENDEN university of applied sciences
MCAD Maritime Cyber Attack Database

- The NHL Stenden Maritime IT Security research group compiled data on **160+ maritime cyber incidents** using open-source information for the MCAD.

- The database covers cyber incidents dating back to 2001, affecting vessels, ports, and other maritime facilities worldwide.

Relevance of AOIP

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

AOIP: closer cooperation to better face challenges and seize opportunities arising from the current and future regional and global environment

Areas of cooperations: Maritime, Connectivity, Sustainable Development Goals

Towards Stronger Cooperation

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

- Enact national laws criminalizing cyber-attacks against critical maritime infrastructure
- Harmonize national cybersecurity laws for maritime transport systems
- Conduct regular maritime cybersecurity drills and exercises
- Establish a national point of contact for maritime cyber incidents
- Create a national coordinating agency for maritime cybersecurity
- Strengthen public–private partnerships with shipping, ports, and energy sectors
- Enhance regional information-sharing platforms (e.g., IFC)
- Ensure effective implementation of IMO cybersecurity guidelines
- Improve coordination between defence agencies, maritime law enforcement and other relevant stakeholders (whole of government approach)

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 (ASEAN)	• 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

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

THANK YOU FOR YOUR KIND ATTENTION