CIL

CENTRE FOR INTERNATIONAL LAW
National University of Singapore

ENHANCING MARITIME SITUATIONAL AWARENESS: ADDRESSING EMERGING CYBER THREATS AND FUTURE CHALLENGES

Dr. Su Wai Mon

Research Fellow

Centre for International Law

National University of Singapore

su.wm@nus.edu.sg

5th Maritime Situational Awareness Working Group (MSA WG) Meeting by MARSEC COE ,15 October 2025

Maritime Security Threat Categories

Category	Examples	Relevant Legal Framework
Traditional Security Threats	Naval warfare, armed conflict	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 boundary disputes	UNCLOS, IMO Conventions

Emerging Security Domains

Domain	**Relevance to Maritime Security**
Land	Port hinterlands, logistics chains, and supporting infrastructure
Sea	Offshore installations, subsea cables, shipping routes
Air	Drones, aerial surveillance, and maritime patrol systems
Cyber/Digital	IT/OT systems in ships and ports, data networks, automation systems
Space	Satellite communication, positioning, and navigation systems (GNSS)

Key Maritime Infrastructure

Infrastructure Type	Examples / Components
Ships	Merchant vessels, naval ships, autonomous vessels
Ports	Terminals, cargo handling systems, port community systems
Offshore Structures	Oil and gas platforms, wind farms, subsea operations
Critical Underwater Infrastructure (CUI)	Submarine communication cables, energy pipelines

CYBERSECURITY OF MARITIME INFRASTRUCTURES

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore

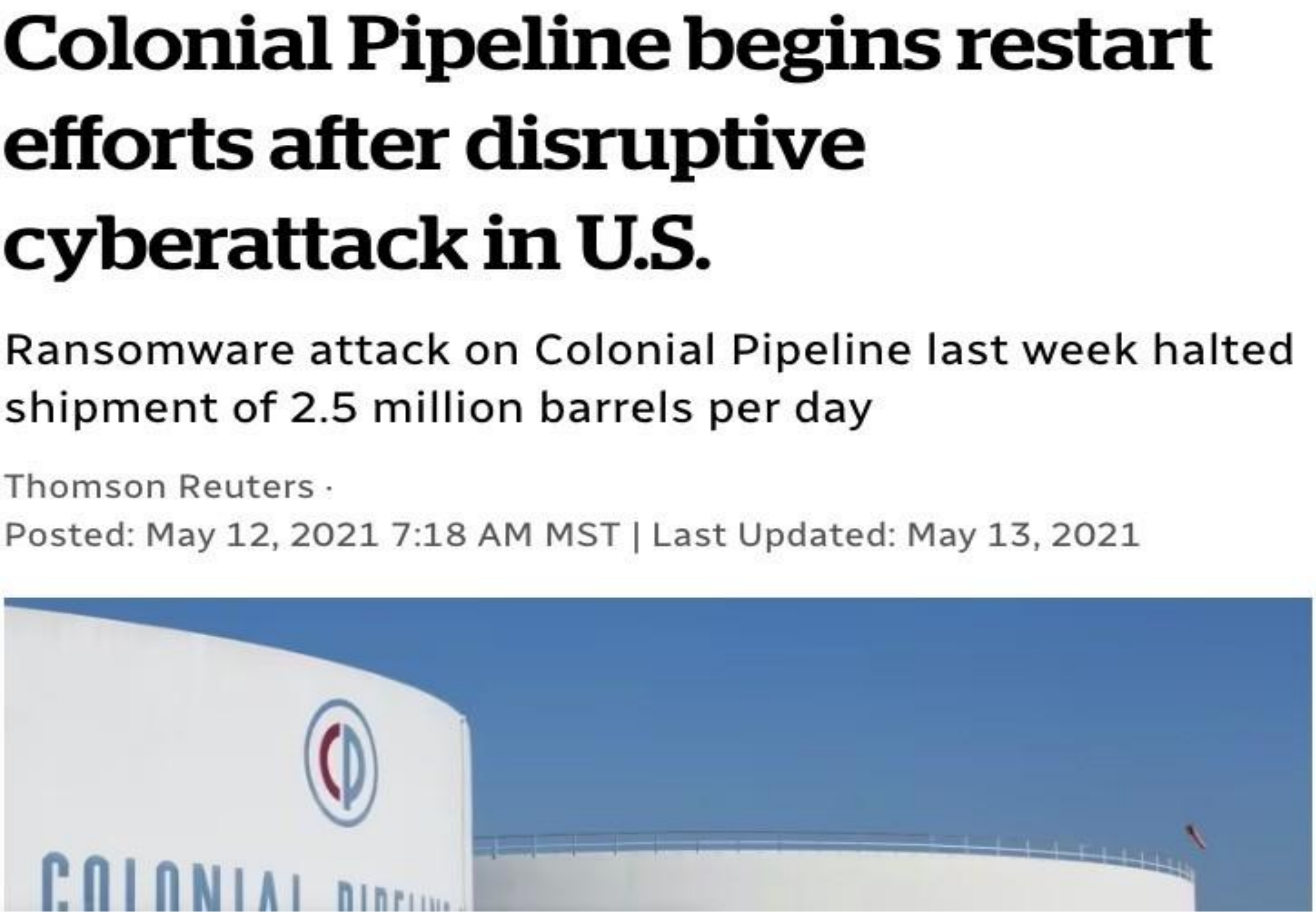
MARITIME CYBERSECURITY

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**

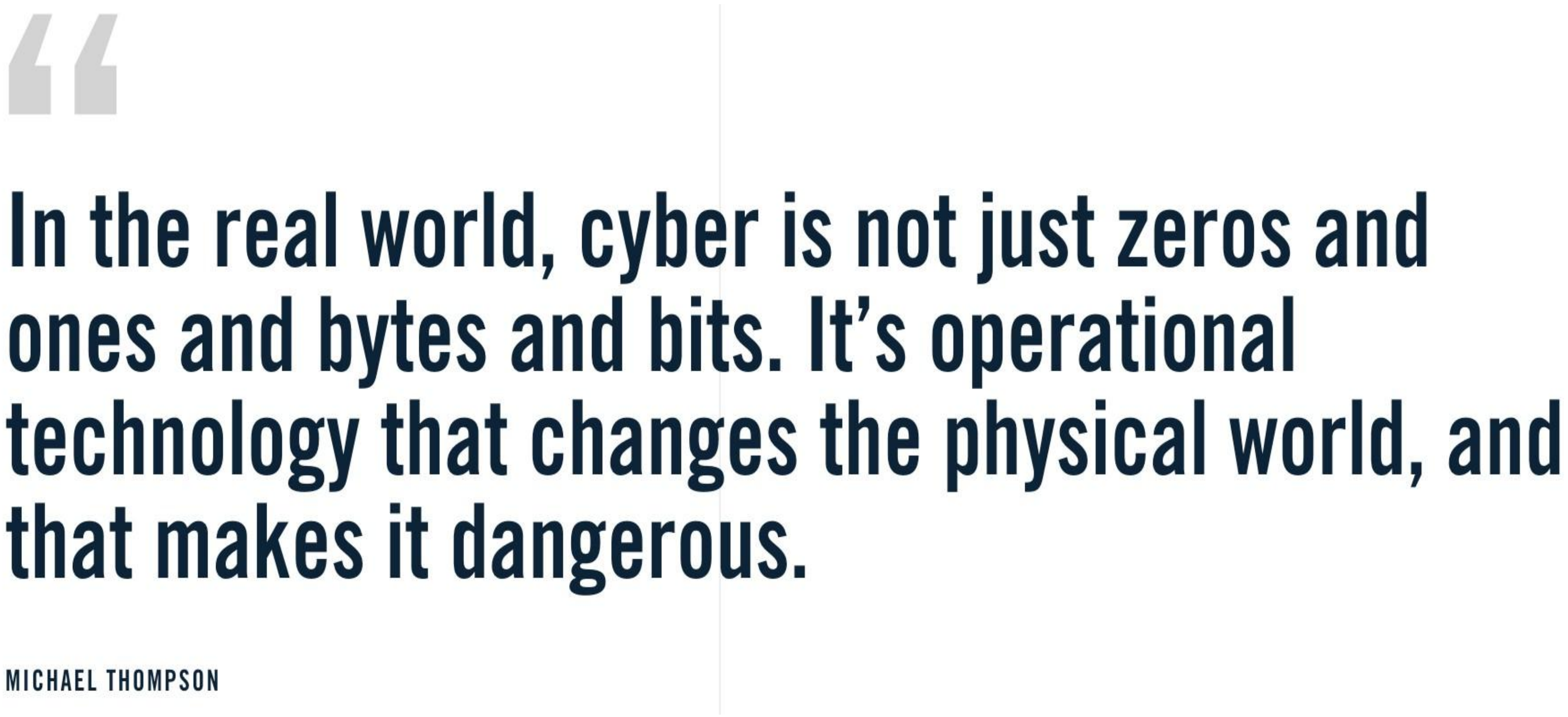
- According to Britannia P&I Club, global costs from cybercrime predicted to exceed **<u>USD 10 trillion by 2025.</u>**
- Although shipping contributes a small part of this total, cyber attacks in the maritime industry now <u>cost the targeted organisation an average of **USD 550,000**</u>**.**



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



> “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)

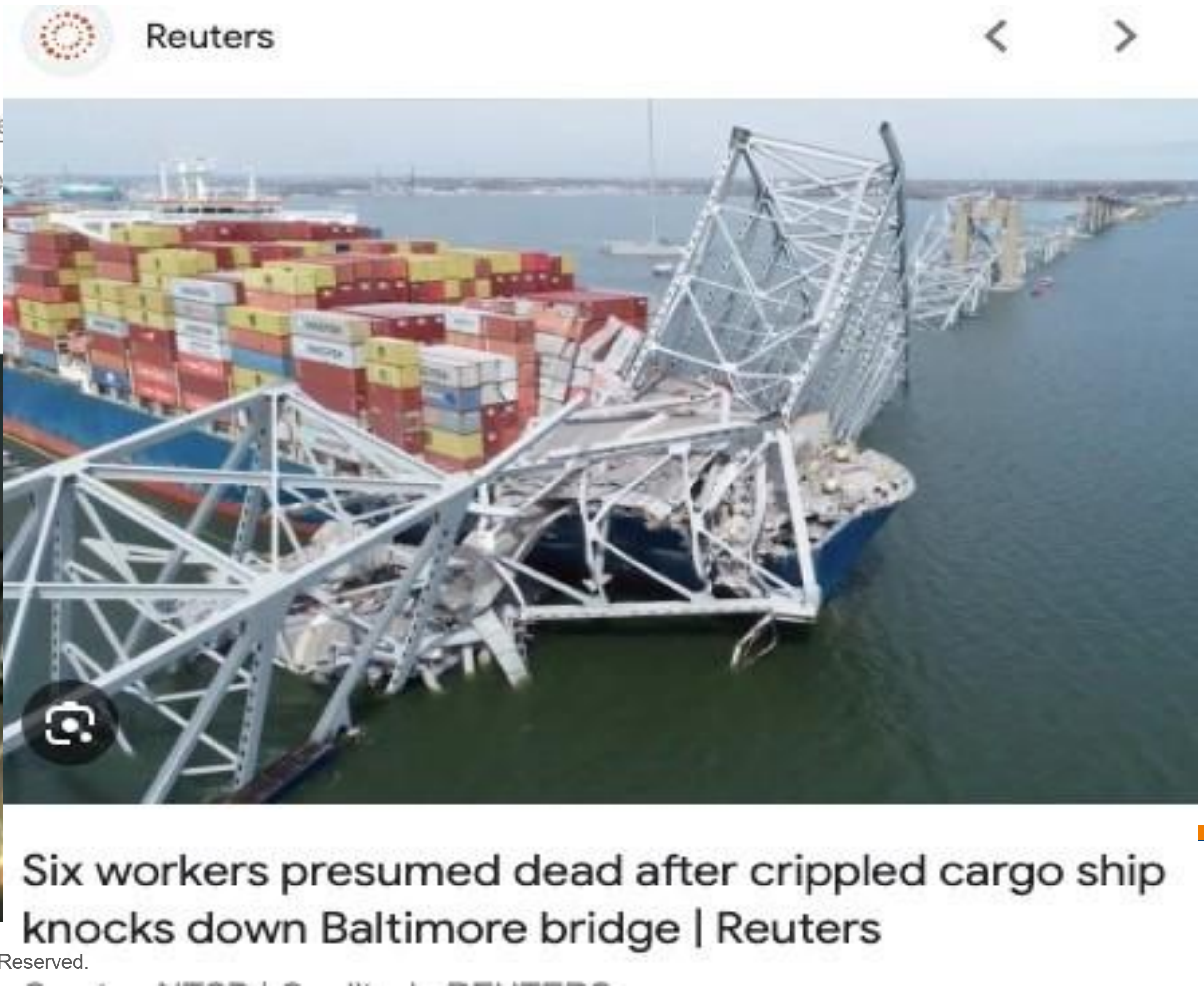
CRISIS SCENARIOS

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

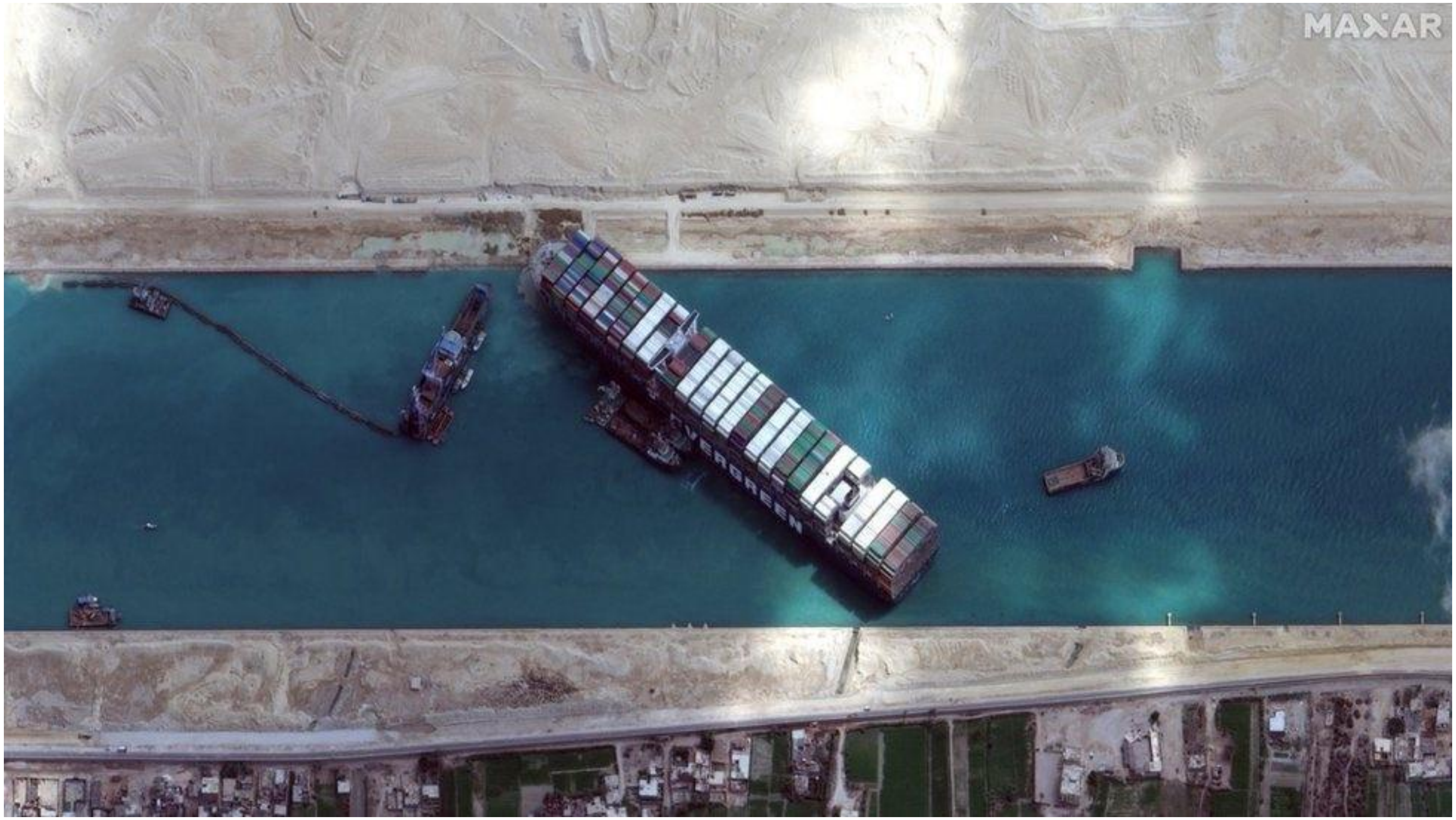


Reuters

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

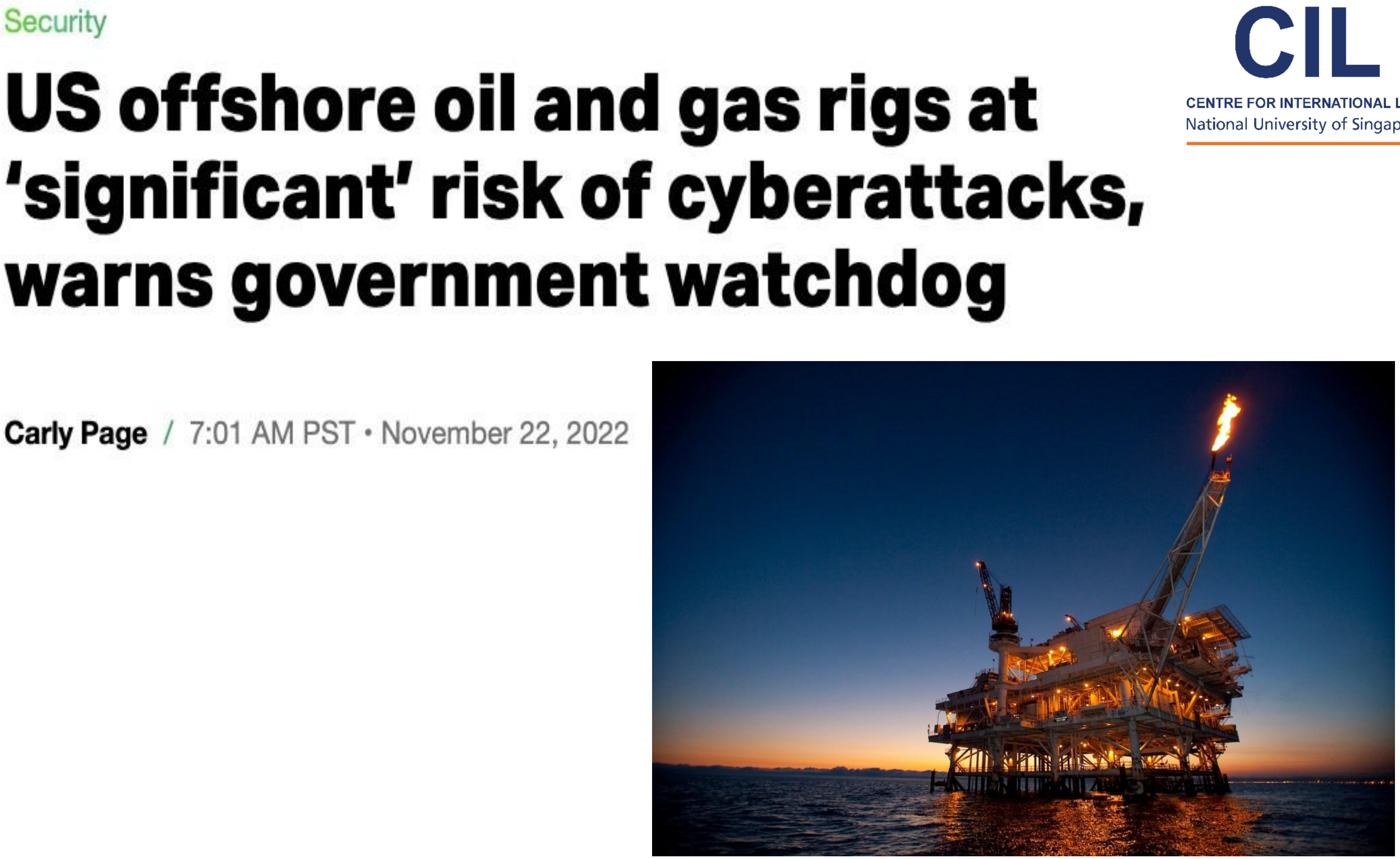
A SATELLITE PHOTOGRAPH REVEALS HOW THE EVER GIVEN WAS WEDGED ACROSS THE CANAL (SOURCE :BBC NEWS)

CIL
CENTRE FOR INTERNATIONAL LAW
National University of Singapore



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

BP Oil Spill Environmental Impact

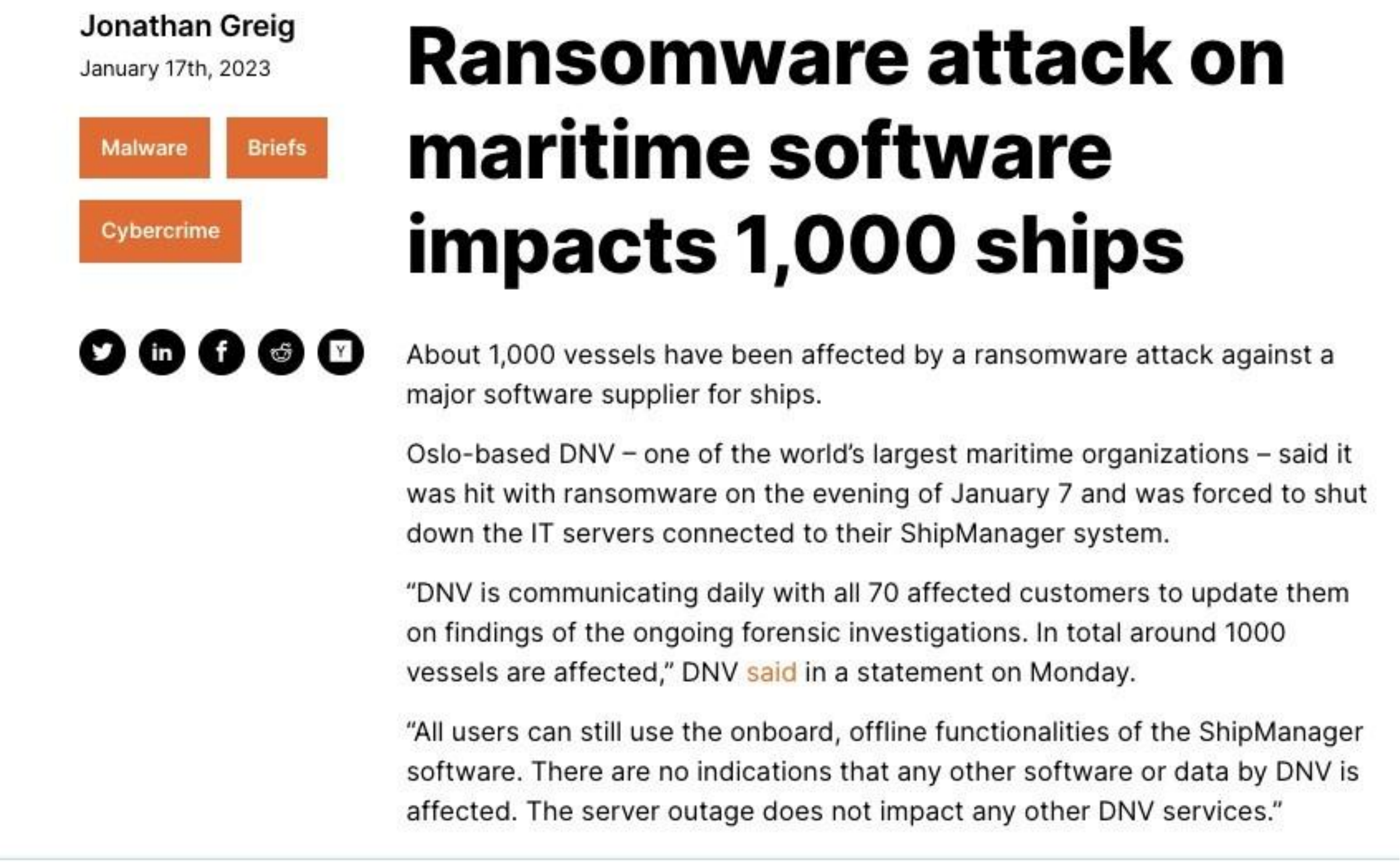


Security

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

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

REPORTED INCIDENTS



Jonathan Greig
January 17th, 2023

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."

CIL

CENTRE FOR INTERNATIONAL LAW

TECHNOLOGY

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

Ransomware shuts down Toyota's export hub

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

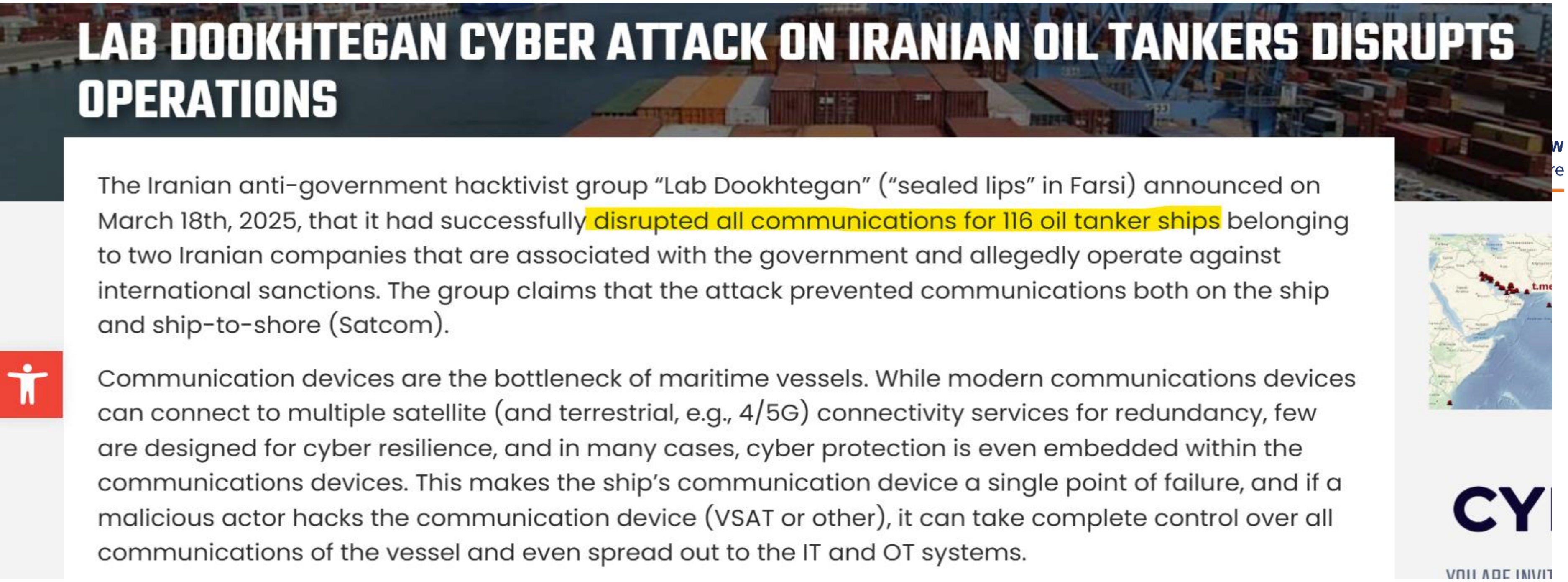
By Dom Magli

TWITTER FACEBOOK LINKEDIN EMAIL

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

February 22, 2022

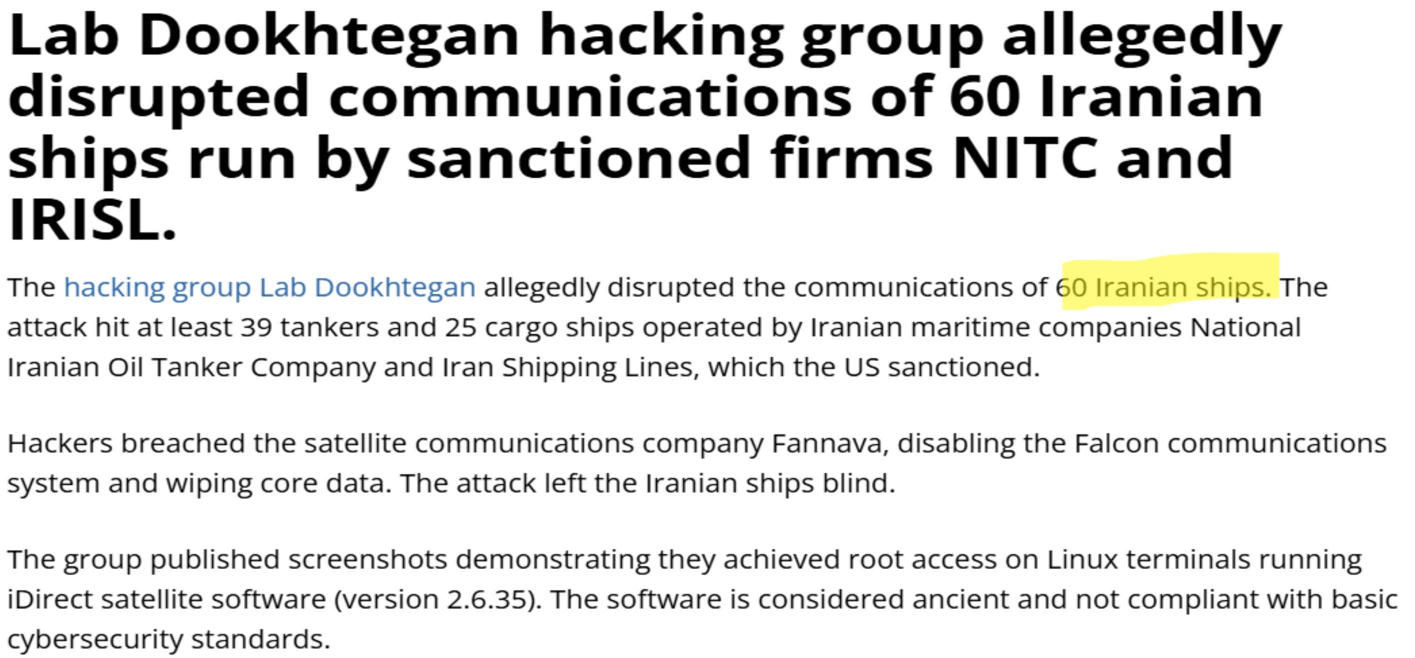
Facebook Twitter Linkedin Email



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.

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

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

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Published by CCDCOE

Policy Brief
Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure

- ✓ Revision of the NATO Alliance Maritime Strategy
- ✓ Establish and Actively Participate in Structured Threat Intelligence-Sharing Networks
- ✓ Establish Dedicated Liaison Roles and Coordination Mechanisms
- ✓ Develop Maritime Cybersecurity Working Groups

It provides an overview of the challenges of digitalisation in the maritime sector demanding coordination between the traditional industrial control systems and contemporary digital solutions; the threat landscape from state-sponsored advanced persistent threats to financially motivated cybercriminals and the policy gaps in current cybersecurity frameworks.

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.

THANK YOU FOR YOUR KIND ATTENTION