OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

Maritime Cyber Crimes

20 July 2023

John Lee

Managing Director

GRF Asia-Pacific / OT-ISAC

Powered by GLOBAL RESILIENCE FEDERATION

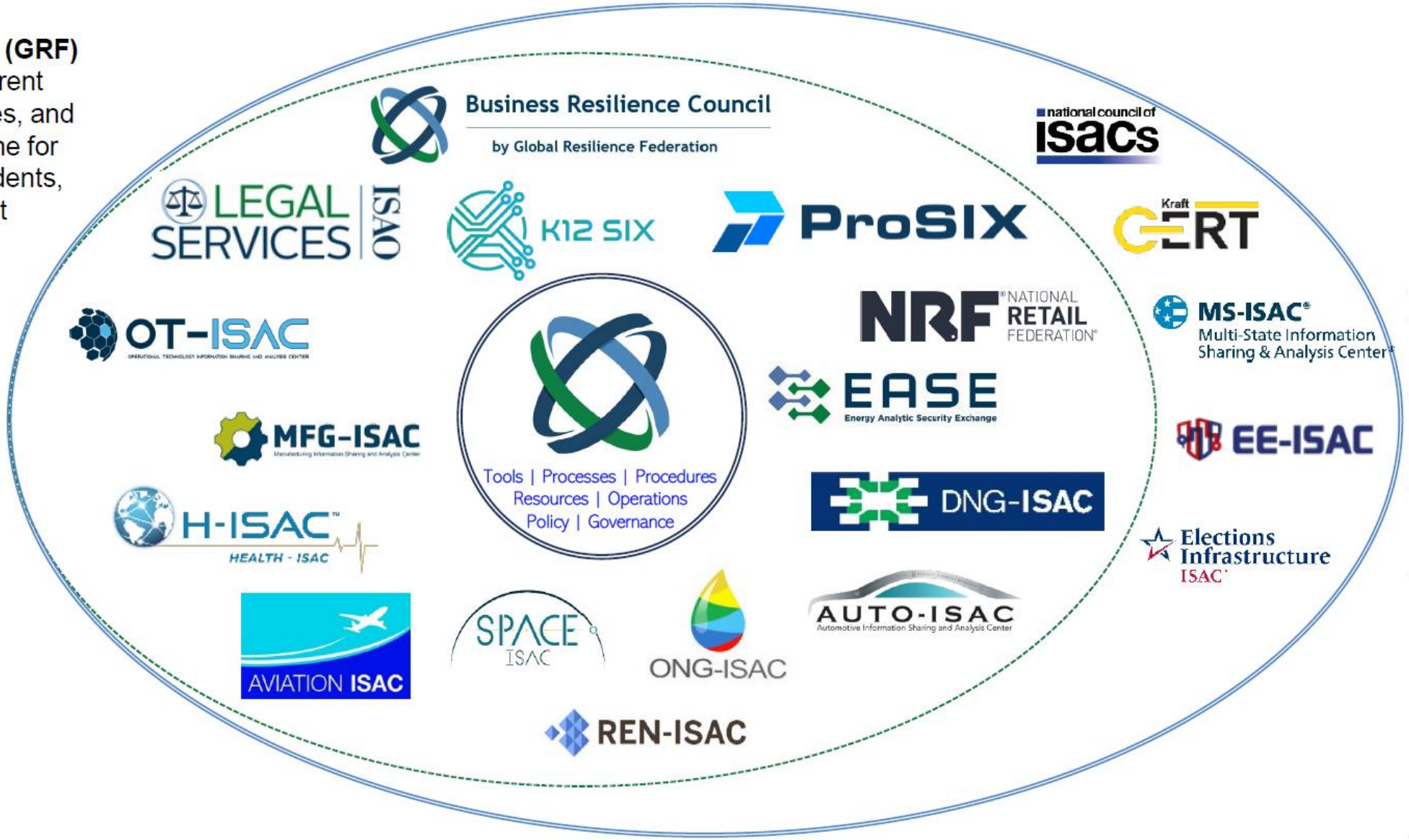
Agenda

- Introduction
- Maritime Cyber threat landscape
- Challenges and Opportunities
- Summary

Introduction

Global Resilience Federation (GRF) manages and supports 17 different information sharing communities, and establishes a common backbone for sharing threat intelligence, incidents, vulnerabilities, policies and best practices.

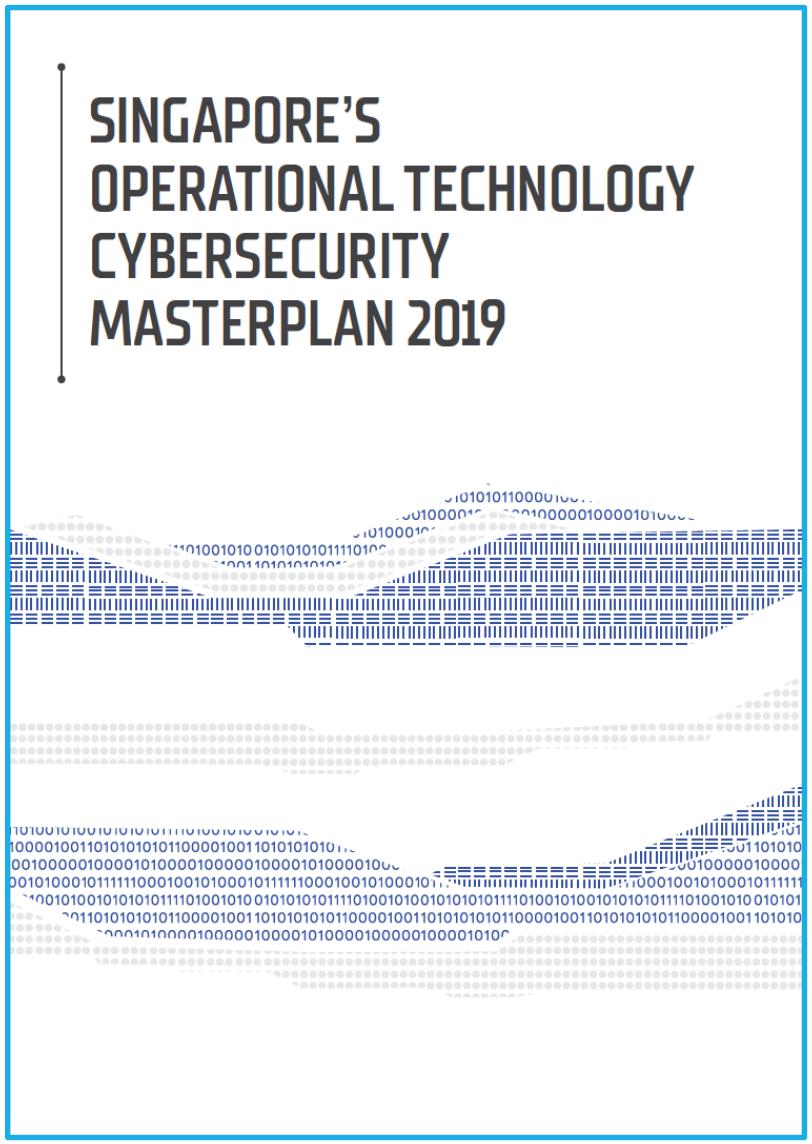
GRF enables cross-sector sharing, enhances situational awareness, and provides tools for collaboration amongst the GRF managed and supported communities.



Introduction

Global Resilience Federation (GRF) is a nonprofit corporation that develops and supports threat information sharing communities and coordinates cross-sector intelligence sharing. In 2014, FS-ISAC established its “Sector Services” department to support non-financial sharing communities. In 2017, that department was renamed Global Resilience Federation and spun out as an independent corporation.

Singapore OT Cybersecurity Masterplan and the code of practice (CCOP)

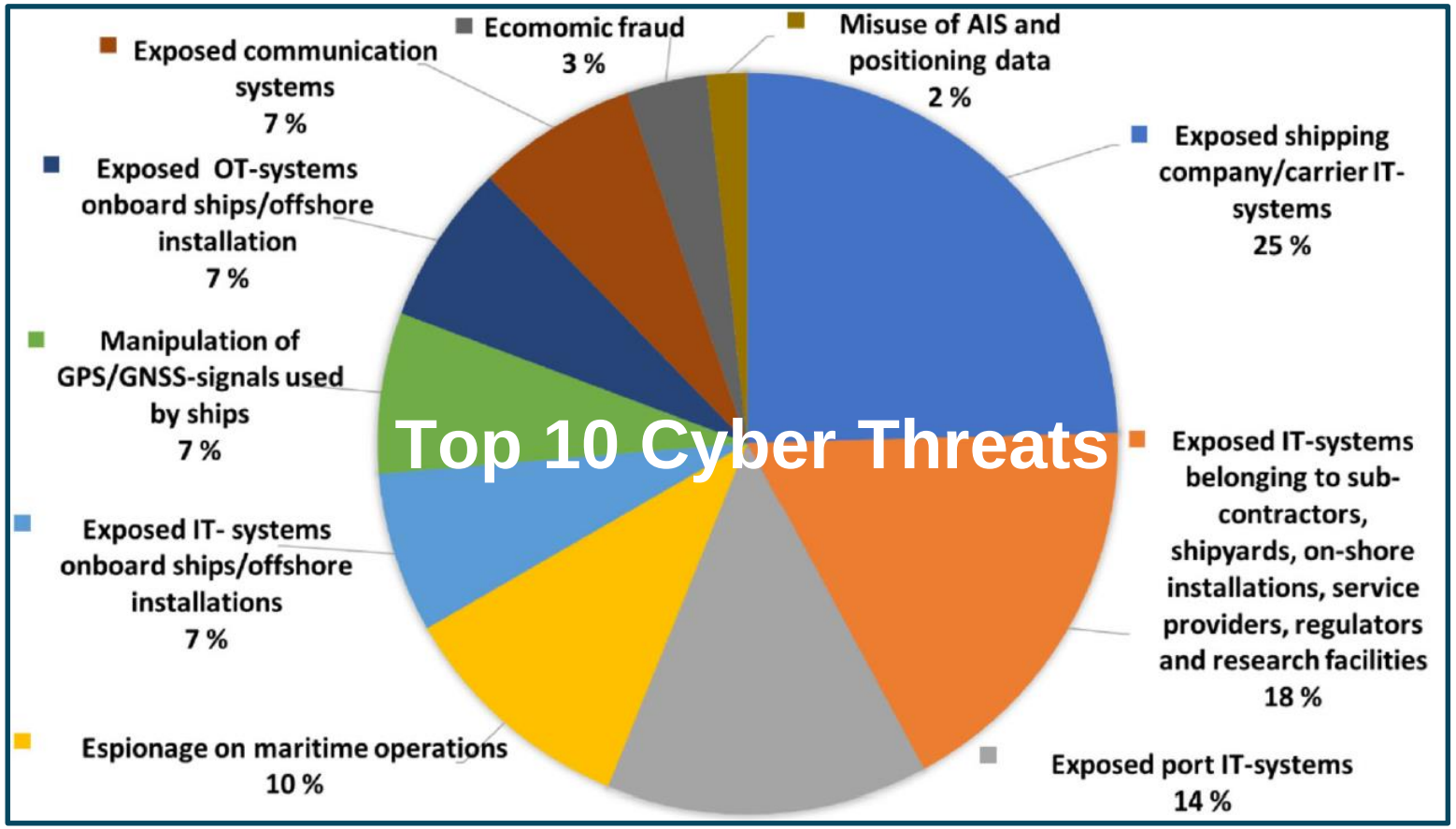


Key thrusts in the OT Cybersecurity Masterplan include:

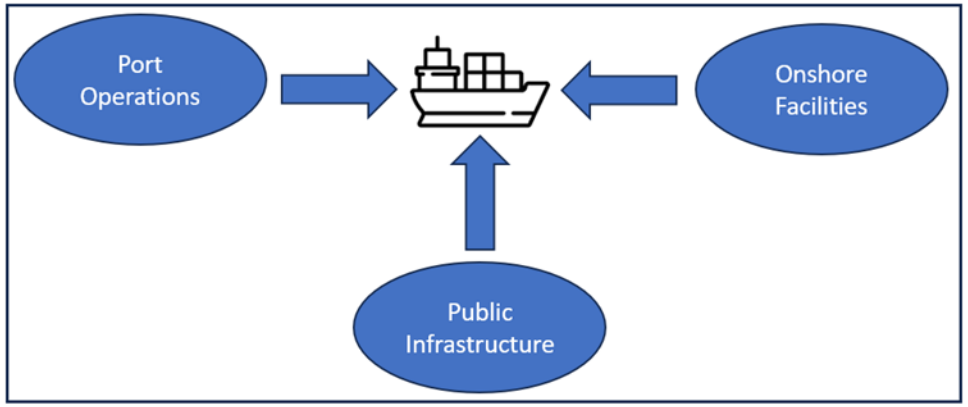
1. Providing OT cybersecurity training to develop human capabilities
2. **Facilitating the sharing of information through an OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC)**
3. Strengthening OT owners' policies and processes through the issuance of an OT Cybersecurity Code of Practice (CCoP)
4. Adopting technologies for cyber resilience through Public-Private Partnerships

Maritime Cyber Threat Landscape

- Last decade has seen rapid introduction of technology and digitization of services
- Organized criminal networks are becoming more sophisticated and targeting onshore facilities, shipping companies and vessels.



Types of Attacks targeting



A Retrospective Analysis of Maritime Cyber Security Incidents, TransNav, International Journal on Marine Navigation and Safety of Sea Transportation. 2021,

Maritime Threat Actors

S/N	Threat Actor	Goal	Technological Level (TL)
1	Generic hackers	Spreading malware on the internet	1
2	Amateur hackers	Improving hacking skills	2
3	Ethical hackers	Finding vulnerabilities to improve security	2
4	Malicious Insider	Revenge or financial gain	3
5	Malicious external providers	Theft of data	3
6	Activists (Hacktivists)	Mission that is not aligned with shipping companies	3
7	Criminal Hackers	Theft of physical cargo, ship or seeking of financial reward	4
8	Competitors	Stealing data or disruption of operations	4
9	Terrorists	Damage ships, infrastructure with intent to cause harm and loss of lives	4
10	Criminals	Transfer of illegal cargo or people	4
11	State Sponsored	Damage or taking control of ship and facilities	5

A Novel Cyber Risk Assessment method for ship systems, Safety Science Journal 131 (2020)

Cyber Attacks on Ports

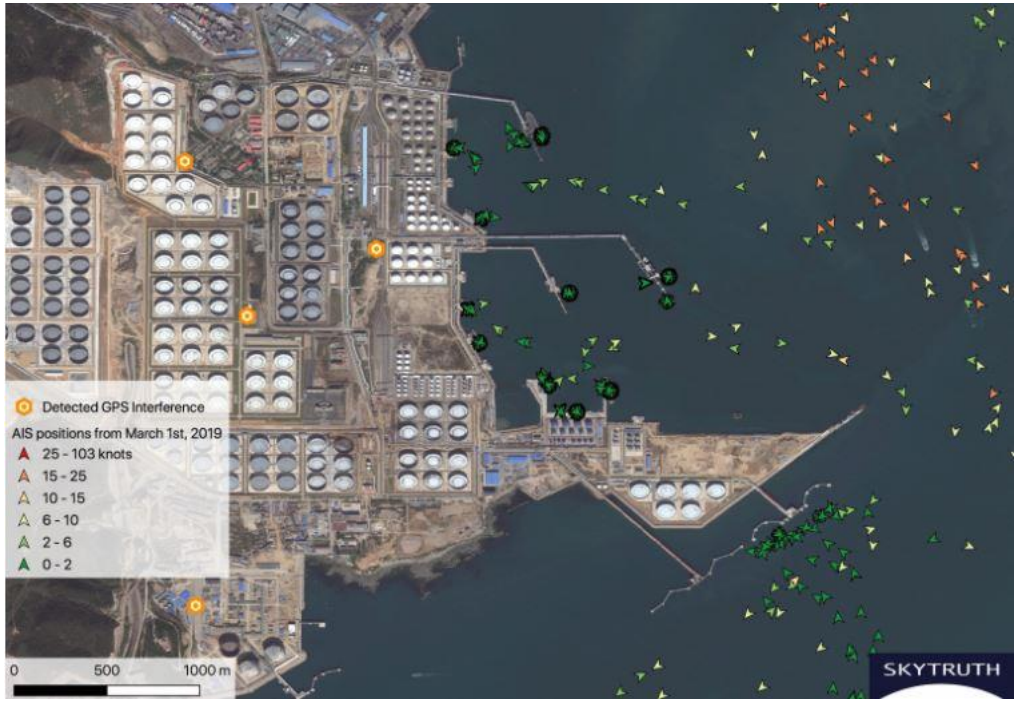
1. **July 2023: Port of Nagoya, Japan**, **suffered a ransomware attack by the Lockbit group.** Nagoya is Japan's busiest port, essential for car exports and critical to the Japanese economy. he attack targeted the port's computer system handling shipping containers and caused a shutdown, disrupting container reception for two days.
2. Other similar incidents occurred at the **Port of Lisbon and multiple ports in Canada**.
3. **January 30, 2022: Conti Ransomware Gang, Gold Ulrick, targeted Belgian port organization's IT systems using Conti ransomware**. The motive was financial gain. Impact: 24 seaports across Europe and Africa affected, including six oil terminals in Antwerp, Ghent, Terneuzen, and Amsterdam leaving operations suspended, leading to oil flow disruptions in the Netherlands, Belgium, and Germany.

Supply Chain Attacks

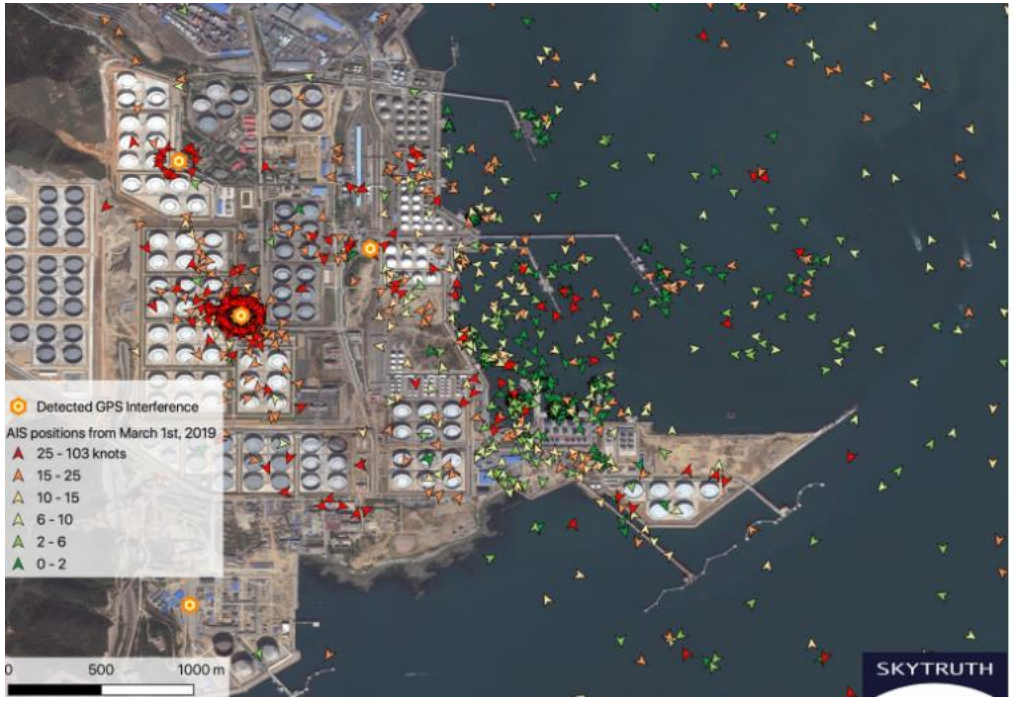
- Ransomware attack on DNV ShipManager servers on 7 Jan 2023. Shipmanager provides solutions to support management of vessels and fleets technically and operationally
- Voyager Fleet insight (VFI) platform was hit by a cyber-attack in December 2022. All systems were taken offline. VSI tracks vessels' navigational activities.

GPS Spoofing

- AIS spoofing observed in an Oil Terminal in Dalian,
- Disrupt vessel tracking in response to sanctions against oil imports from Iran
- Pictures below taken on 2 different dates



BEFORE (1 March 2019)



AFTER (5 September 2019)

https://skytruth.org/2019/12/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations/

Hackers compromise port operations for drug activities

- Port of Antwerp and Port of Rotterdam hacked from 2011 to 2013
- Hackers were working for a drug cartel use spear-phishing attacks with Trojan attachments, installation of key-logging devices to attack 2 container terminals
- The purpose was to track and manipulate container locations for drug pick-ups
- Disappearance of containers (mostly containing drugs), port paid €200,000 for countermeasures
- Cocaine Seizures: 250kg seized leaving Antwerp for Holland, 114kg discovered in April
- Total Seizures: Illicit drugs and contraband worth approximately US$ 365 million, firearms worth approximately US$ 1.5 million
- A dozen suspects were arrested
- Total Drug Seizures: 1044 kilos of cocaine and 1099 kilos of heroin seized by authorities.

https://www.bbc.com/news/world-europe-24539417

Ransomware attacks on Shipping Company

- In March 2023, Dutch maritime logistics company Royal Dirkzwager confirmed being hit with ransomware by the Play group.
- The Play ransomware group previously targeted government entities in Latin America since July 2022. The group gained notoriety for a damaging attack on the City of Oakland, which took weeks to recover from.
- The ransomware attack on Royal Dirkzwager did not impact its operations, but data theft occurred from servers containing contracts and personal information.

https://therecord.media/royal-dirkzwager-ransomware-attack-dutch-shipping

Challenges and Opportunities facing Maritime digitalization

	Challenges	Opportunities
Automation	Increasing use of Cyber Physical Systems (CPS) open up avenues of atttacks	Increased efficiency in various aspects of shipping and port operations through automation
Regulations	Different flag ship compliance and regulations make it increasingly complex	IMO and BIMCO guidelines for ship cybersecurity
Emerging Technologies	Incorporating emerging technologies into maritime digitalization may present integration challenges	Embracing emerging technologies for improved supply chain transparency
Adopting data driven insights	Digital systems require crew training and adaptation	Collection and analysis of large amounts of data optimizingfuel consumption, route planning and operational efficiencies
Public-Private collaboration	Lack of initiatives, unwillingness to collaborate etc	Foster innovation and standardization in maritime digitalization leading to more robust systems

Summary

1. Implementing best cybersecurity practices using a risk-based approach
2. Collaboration between public and private sectors sharing relevant threat information
3. Fostering community engagement through a trusted channel

Thank you!.

Email: jlee@grf.org
Website: www.otisac.org