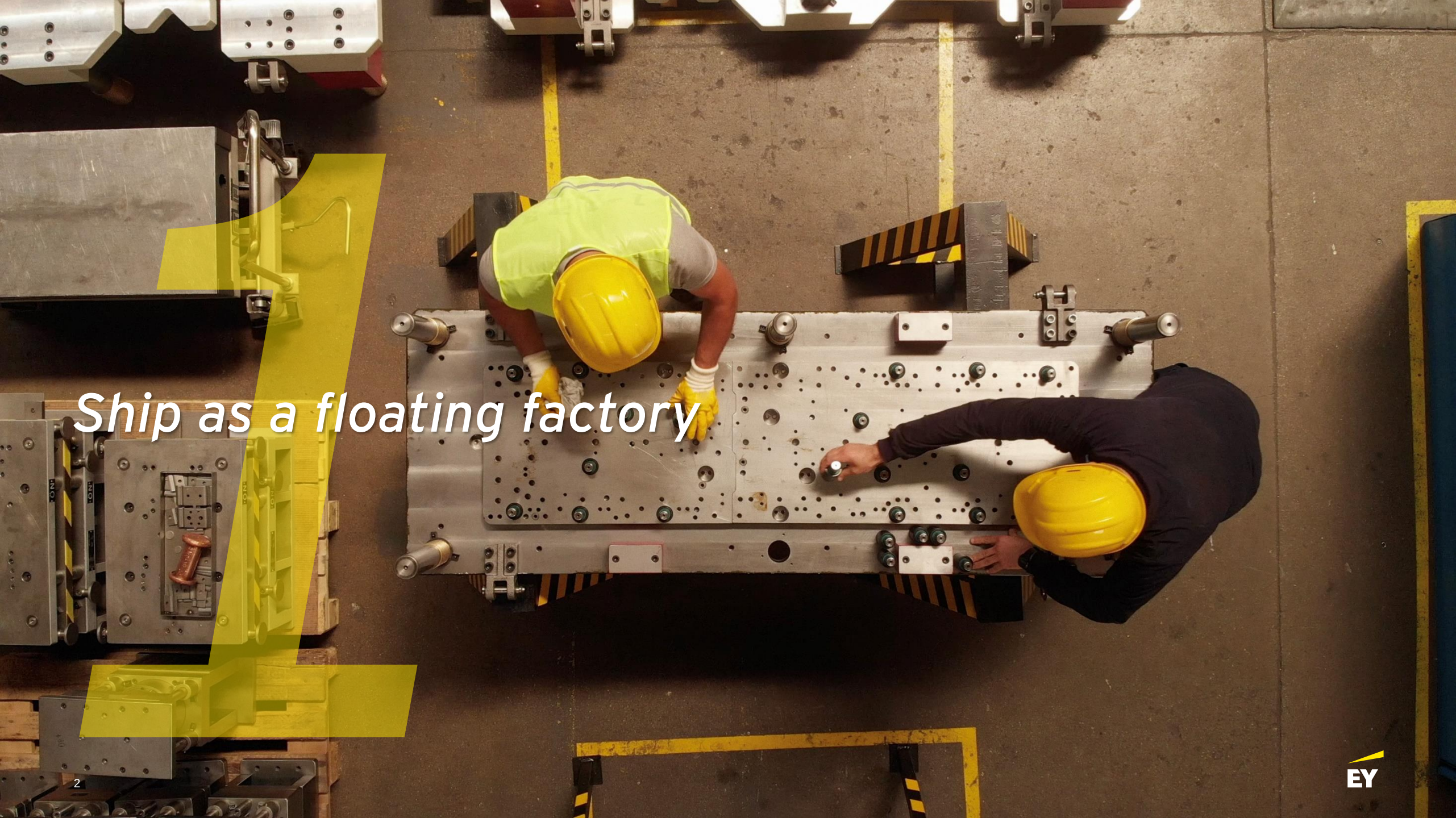
How the maritime cybersecurity threat picture is changing (the world)

Andrzej Gab, Marcin Marciniak – EY Poland

The Digital Ship Conference, Hamburg, Dec 2023

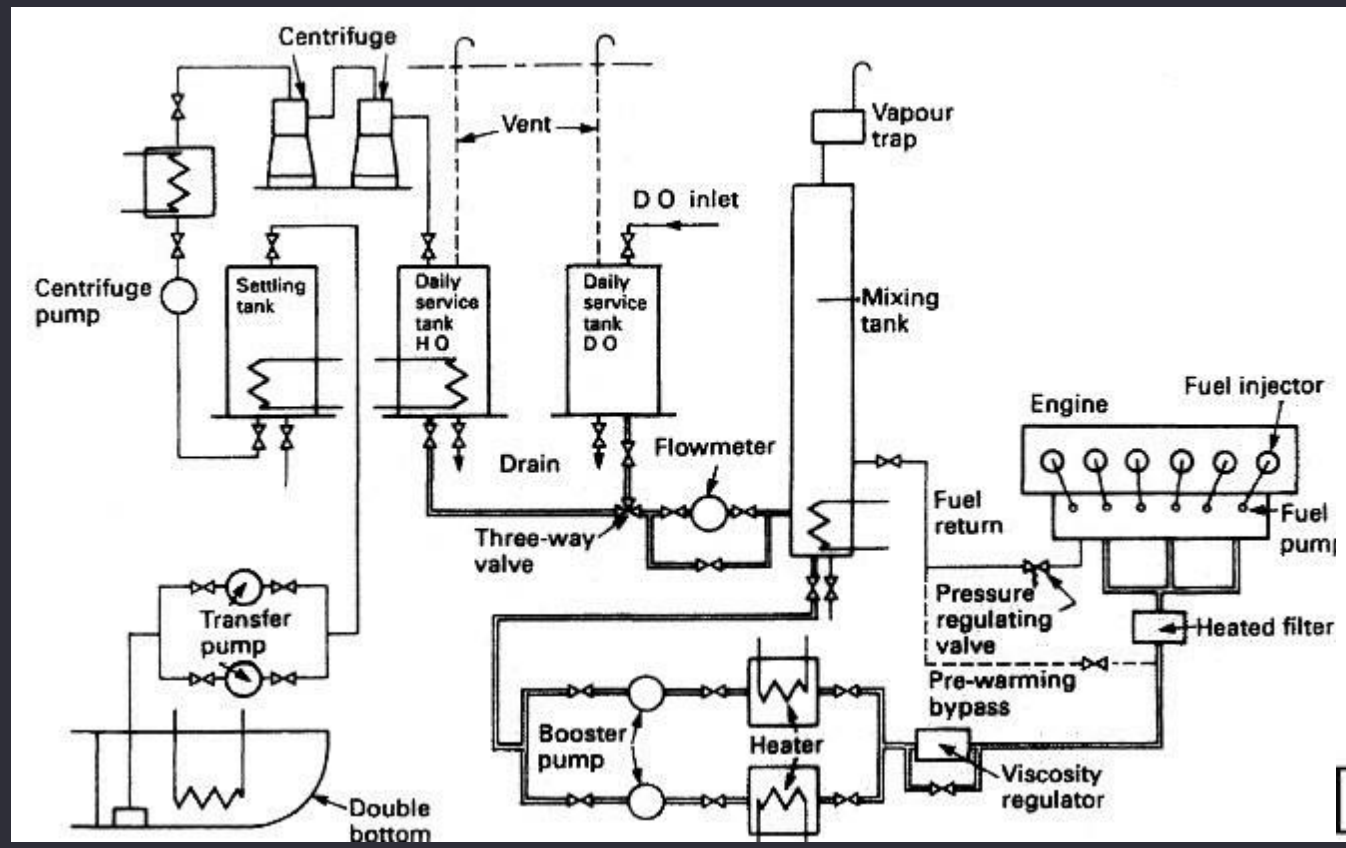
Building a better working world

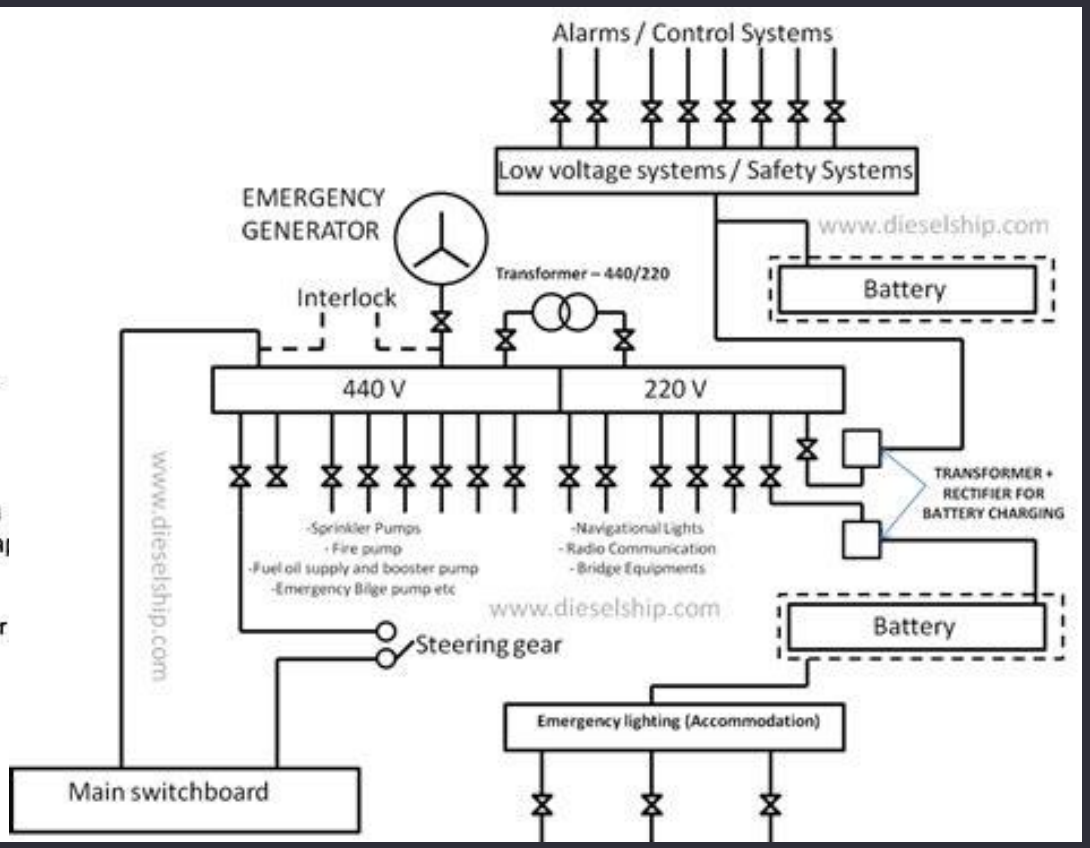


1

Ship as a floating factory

Ship as a floating factory






2
What could happen?

What can happen?

- *An e-mail came, requesting participation in a survey, security related*
- *Computers tend to be a bit slow*
- *Increased amount of external traffic observed on the firewall*
- *One gate opened by itself, can't be closed*
- *All of the port gates are open, including bonded store*
- *ID cards don't work, persons can't enter the building*
- *Power supply problems, cranes don't work*
- *A small fire in the port facilities*
- *Port Community Systems do not respond, cargo documents can't be printed or sent*
- *Ransom ($250k) request message is displayed on all PCs*
- *Could it happen?*

It has already happened. At least in part.

Port of Barcelona Suffers Cyberattack

By Ionut Ilascu

Ransomware attack hits Port of San Diego

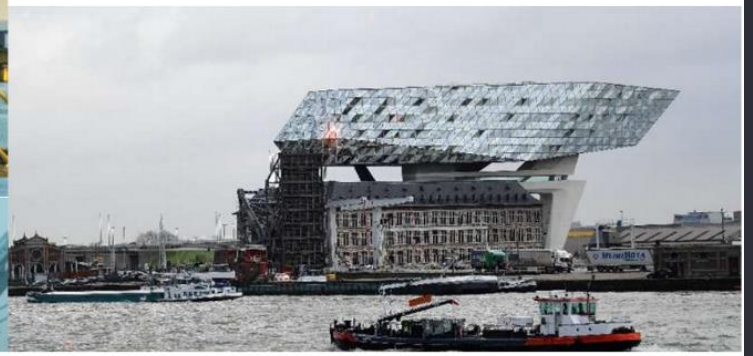
There's no safe harbor here.

Alfred Ng
Sept. 28, 2018 10:36 a.m. PT
2 min read

FEBRUARY 3, 2022

European oil port terminals hit by cyberattack

By Matthieu Demeestere With Afp Bureaux



Ransomware attack takes US maritime base offline

2 January 2020

What Happened?

The Shahid Rajaee port facility is the newest of two major shipping terminals in the Iranian coastal city of Bandar Abbas, on the Strait of Hormuz. Computers that regulate the flow of vessels, trucks and goods at the port were knocked offline simultaneously on May 9, 2020, disrupting operations and causing road and waterway congestion that lasted several days.

3

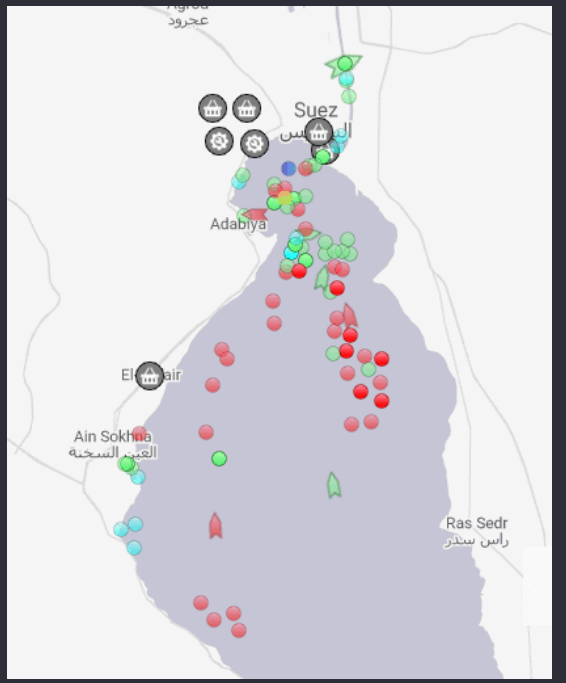
What about ships?

Ship enters port – what could go wrong?

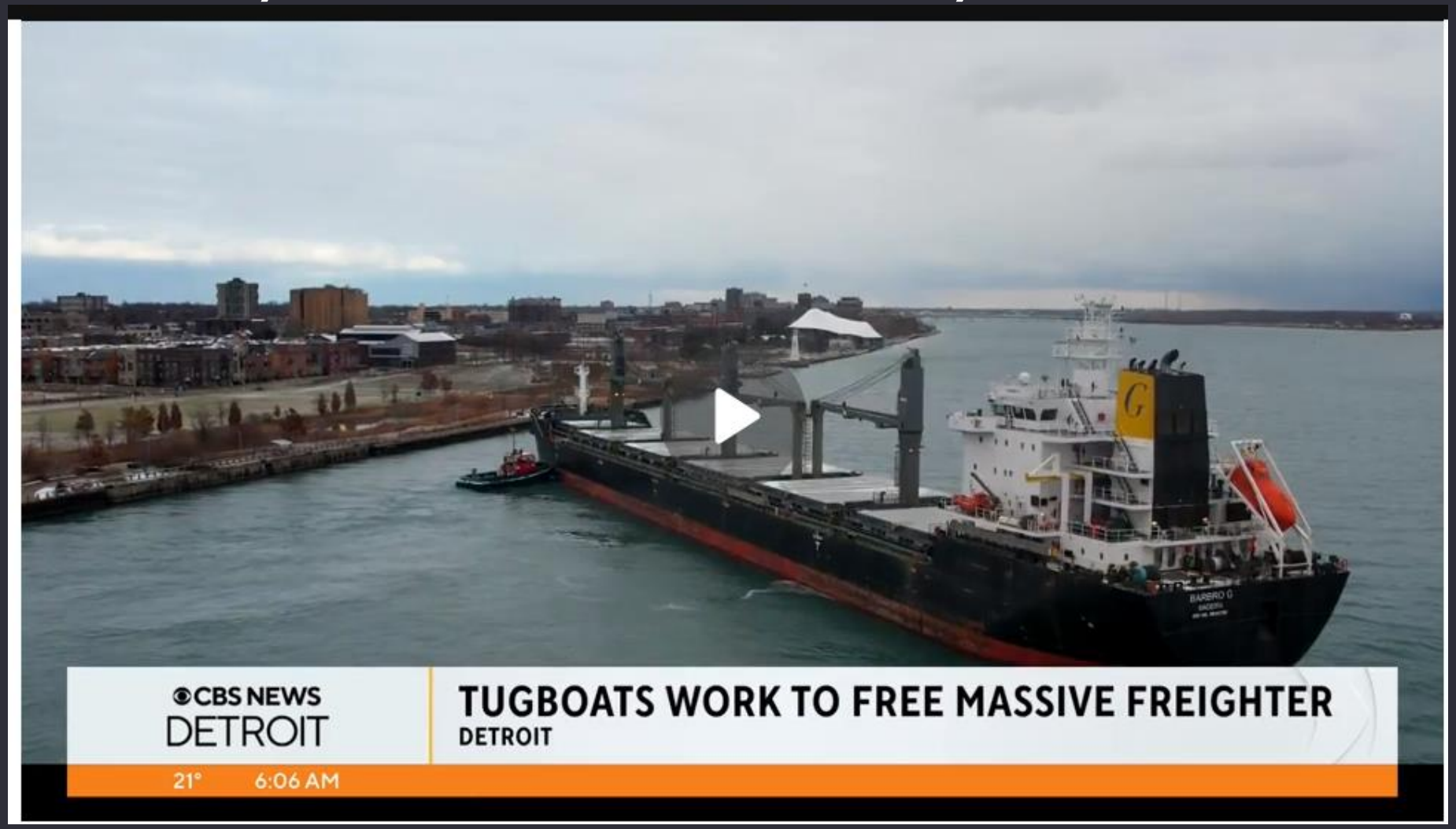
- *Another e-mail came, requesting update to the digital maps on the bridge systems*
- *Update executed successfully, no problems observed*
- *Master requests pilot before entering a channel to the port*
- *Dead slow ahead, as planned. Master informs on small problems with digital maps*
- *Ship is progressing slowly, other ship reports similar problems with maps*
- *Ships declares mayday, engine flank ahead, helm hard to port, thrusters don't work*
- *Ship hits the pier at 6kts*
- *What could be the worst outcome?*

What is the cyber attach possible impact?

- *Case of the m/v Ever Given/H3RC, IMO 9811000*
- *This can happen to any tanker or freighter as a result of cyberattack*



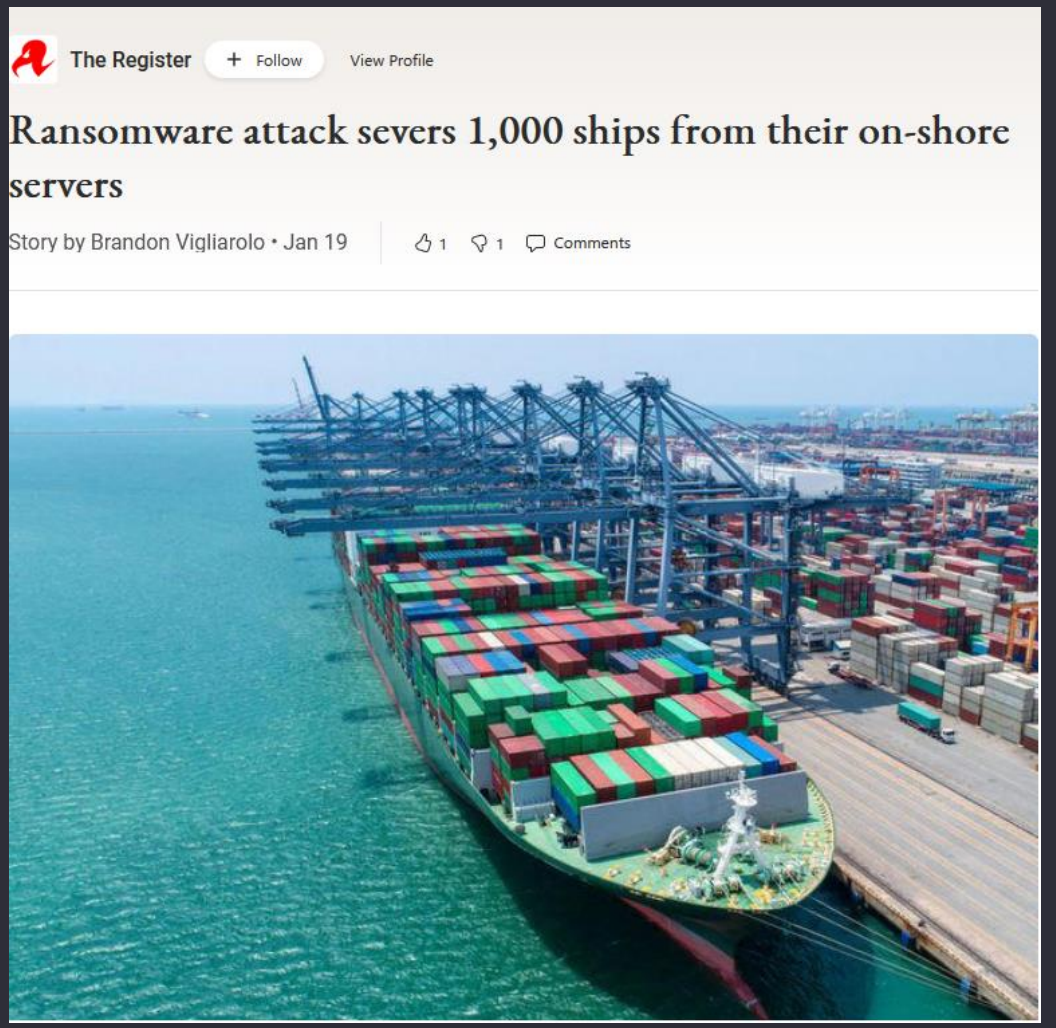
It's not Cyber related. At least not yet. But it could be.



"Barbro G" IMO 9546796, c/s CQOW, QTH: Detroit River

It is all connected!

- *Port systems "can see" multiple vessels*
- *Ship-ship communication (e.g. LNG bunkering from LBV)*
- *Possible malware spread:*
  - *Both directions*
  - *Custom malware pointing against industry software (such as ShipManager)*
  - *Can infect or disable or malfunction OT as well*
- *Possible impact:*
  - *Service outage impacting multiple ships*
  - *Further lateral movement – other systems infected*

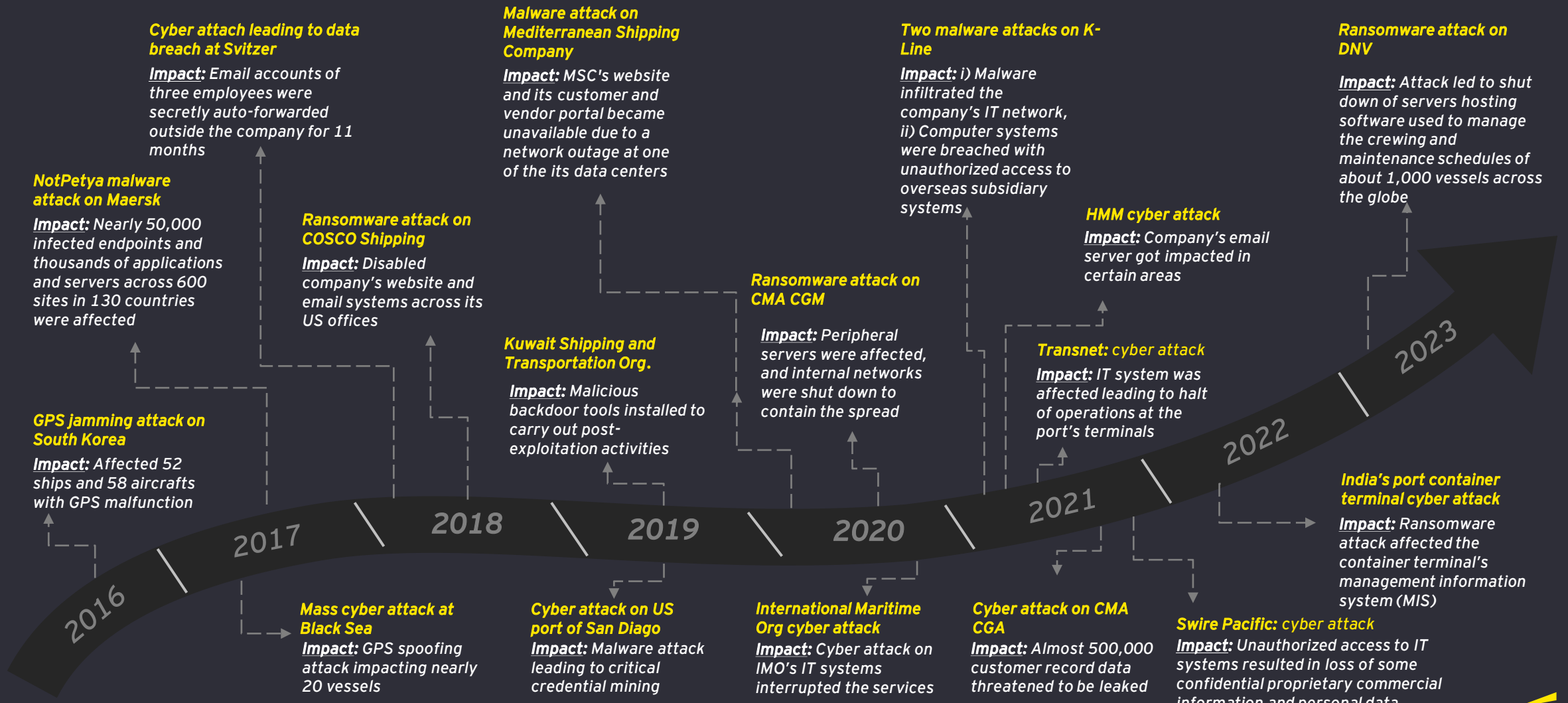


- *https://www.msn.com/en-us/news/technology/ransomware-attack-severs-1000-ships-from-their-on-shore-servers/ar-AA16vMbu*


4
Problem is global

Attacks timeline

Some major cyber attacks over the years



NotPetya malware attack on Maersk

Impact: Nearly 50,000 infected endpoints and thousands of applications and servers across 600 sites in 130 countries were affected

GPS jamming attack on South Korea

Impact: Affected 52 ships and 58 aircrafts with GPS malfunction

Cyber attach leading to data breach at Svitzer

Impact: Email accounts of three employees were secretly auto-forwarded outside the company for 11 months

Ransomware attack on COSCO Shipping

Impact: Disabled company's website and email systems across its US offices

Mass cyber attack at Black Sea

Impact: GPS spoofing attack impacting nearly 20 vessels

Malware attack on Mediterranean Shipping Company

Impact: MSC's website and its customer and vendor portal became unavailable due to a network outage at one of the its data centers

Kuwait Shipping and Transportation Org.

Impact: Malicious backdoor tools installed to carry out post-exploitation activities

Cyber attack on US port of San Diago

Impact: Malware attack leading to critical credential mining

Ransomware attack on CMA CGM

Impact: Peripheral servers were affected, and internal networks were shut down to contain the spread

International Maritime Org cyber attack

Impact: Cyber attack on IMO's IT systems interrupted the services

Two malware attacks on K-Line

Impact: i) Malware infiltrated the company's IT network, ii) Computer systems were breached with unauthorized access to overseas subsidiary systems

HMM cyber attack

Impact: Company's email server got impacted in certain areas

Transnet: cyber attack

Impact: IT system was affected leading to halt of operations at the port's terminals

Cyber attack on CMA CGA

Impact: Almost 500,000 customer record data threatened to be leaked

Ransomware attack on DNV

Impact: Attack led to shut down of servers hosting software used to manage the crewing and maintenance schedules of about 1,000 vessels across the globe

India's port container terminal cyber attack

Impact: Ransomware attack affected the container terminal's management information system (MIS)

Swire Pacific: cyber attack

Impact: Unauthorized access to IT systems resulted in loss of some confidential proprietary commercial information and personal data

Source: Factiva and news articles


5
Sector is unique

What makes maritime security unique?

- *Different than pure IT/OT ashore (even in oil & gas industry),*
- *No direct chain (MASTER responsibility),*
- *Even OT in maritime sector is unique,*
  - *Split responsibility,*
  - *Different maintenance,*
  - *Very long upgrade process (has to match drydocking),*
- *Only satellite links available:*
  - *Satcom links upgrade without updating security posture,*
  - *Remote access,*
  - *Security in transit issues,*
- *Maintenance problem in case of failure.*

- *Real questions:*
  - *Is responsibility over IT and OT split?*
  - *Are superintendents aware of the risk and its mitigation?*
  - *Are the maintenance procedures up to date?*
  - *How general remote access policies look like?*
  - *How data security in transit looks like?*
  - *Is there any monitoring that pushes data to company ashore?*
  - *Is it fed to incident response team?*


The global call

- *What is our business message to maritime company leadership?*

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

XXXXX-XXXGbl
ED MMYY

[Optional environmental statement – refer to The Branding Zone]

ey.com