

ECCWG

Maritime IT Security Research Group

Jeroen Pijpker
Stephen McCombie



university of
applied sciences



About @Jeroen

- Over 15 years experience as a researcher/lecturer
- Getting students ready to become a Certified Ethical Hacker (CEH)
- Teaching students in Secure Programming
- IoT Hacking
- Botnet research



About @Stephen

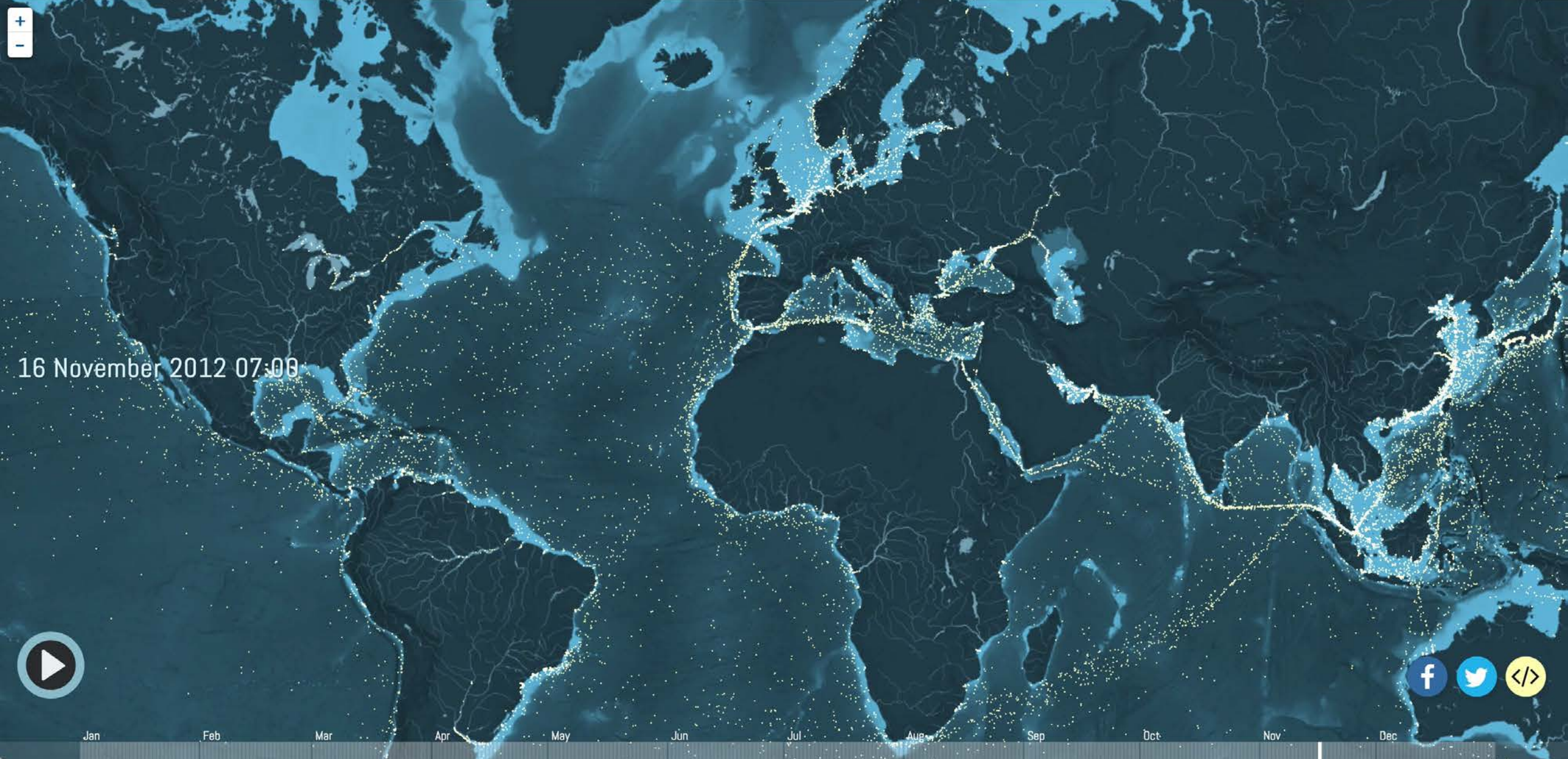
- Over 25 years working in cyber security
- Worked in law enforcement, academia and industry
- PhD in Computer Science - Thesis examined Russian and Ukrainian cybercrime groups that targeted Australian Banks in early 2000s
- Research interests include maritime cyber threats, cyber threat intelligence, state sponsored offensive cyber and information warfare



Maritime Cybersecurity Research Group



- Established September 2021
- Goal is to conduct impactful research into Cyber threats to the Maritime Transportation System (MTS)
- Our scope apart from traditional maritime activities includes inland waters, port facilities and other critical elements of the MTS
- This is achieved by leveraging our skills across disciplines within NHL Stenden in Ethical Hacking, Secure Programming, Serious Gaming, Maritime Technology, Maritime Officer Training, Marine Shipping Innovations and Cyber Safety
- Three major projects



Global Maritime Transportation System

- The role of GMTS in the global economy is significant with over 80% of the world's cargo transported by ship (Bronk & Dewitt 2020) and representing 70% of global trade by value (Loomis & Singh, et al 2021).
- At the same fleets are aging and their technology is aging with them and thus more vulnerable to cyber-attacks. 38% of oil tankers and 59% of general cargo ships are more than twenty years old (Tam and Jones 2018).





(Kessler and Shepard 2022)

Port Components at Risk

1

Facility Access

A compromise impacting physical access control systems can lead to supply chain delays and localized traffic congestion in the vicinity of a port.

2

Terminal Headquarters – Data

Terminal and Gate Operating Systems (TOS/GOS) streamline the flow of cargo in a port. A compromise of a port's TOS/GOS data could result in leaks of sensitive supply chain data from port customers. Manipulation of TOS/GOS data could also be used for smuggling or cargo theft.

3

Terminal Headquarters – Ransomware

A ransomware attack affecting TOS/GOS systems could make critical systems and data inaccessible. This could lead to a full stop of port operations, resulting in financial losses and supply chain disruptions.

4

Operational Technology (OT) Systems

Maritime infrastructure relies on various OT systems to control pumps, cranes, and other industrial equipment. The compromise of an OT system can cause safety issues and lead to loss of life or property. In addition, a compromise can disrupt facility operations.



5

Positioning, Navigation, and Timing (PNT)

PNT often supports many vessels within a port's vicinity, and is critical to maritime operations. Loss of PNT can impede vessels' ability to safely navigate a port, and lead to an increased risk of collisions and groundings. Any of these events can result in environment damage, loss of life or property, or a disruption to safe navigation.

6

Vessel

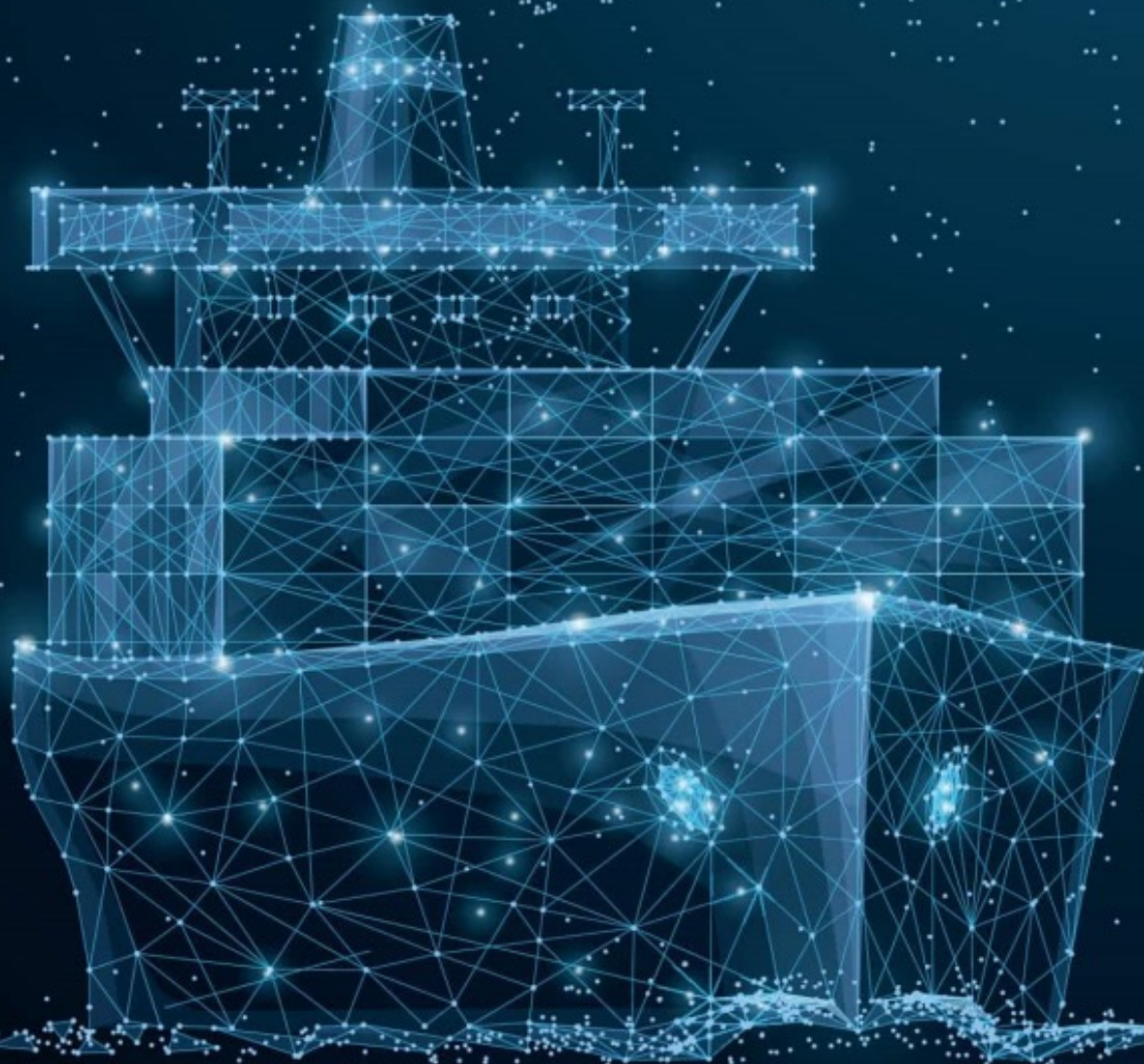
A compromise to shipboard systems could impact a vessel's ability to safely navigate and manage their cargo. A vessel compromise could also lead to disruption of shore-side systems, because lateral movement is possible through shared wireless or wired networks, portable media, and other interconnections.



Database of Maritime Cyber Incidents

- This project involves building a database of all maritime cyber incidents that have occurred where information is available from open sources.
- The database will utilise Structured Threat Information Expression (STIX™), which is a language and serialization format used to exchange cyber threat intelligence (CTI).
- In student projects, data will be collected and a database built, and then maintained and updated.
- The database will have a public online presence and will be used to produce reports and research papers.
- It will also be used as input for simulations and other research.



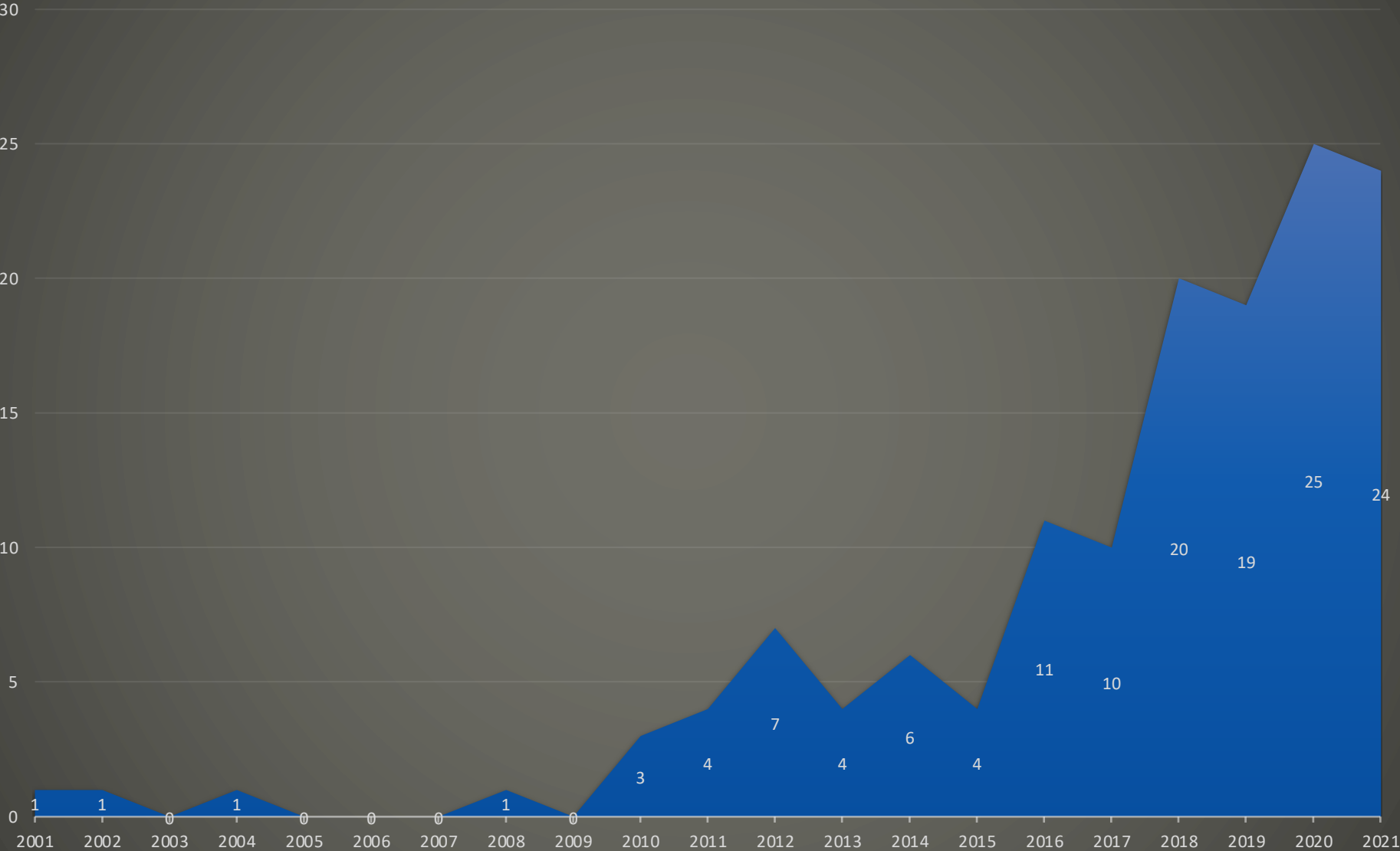


STIX Database

The place for maritime cyber
incidents reporting

Login/Register

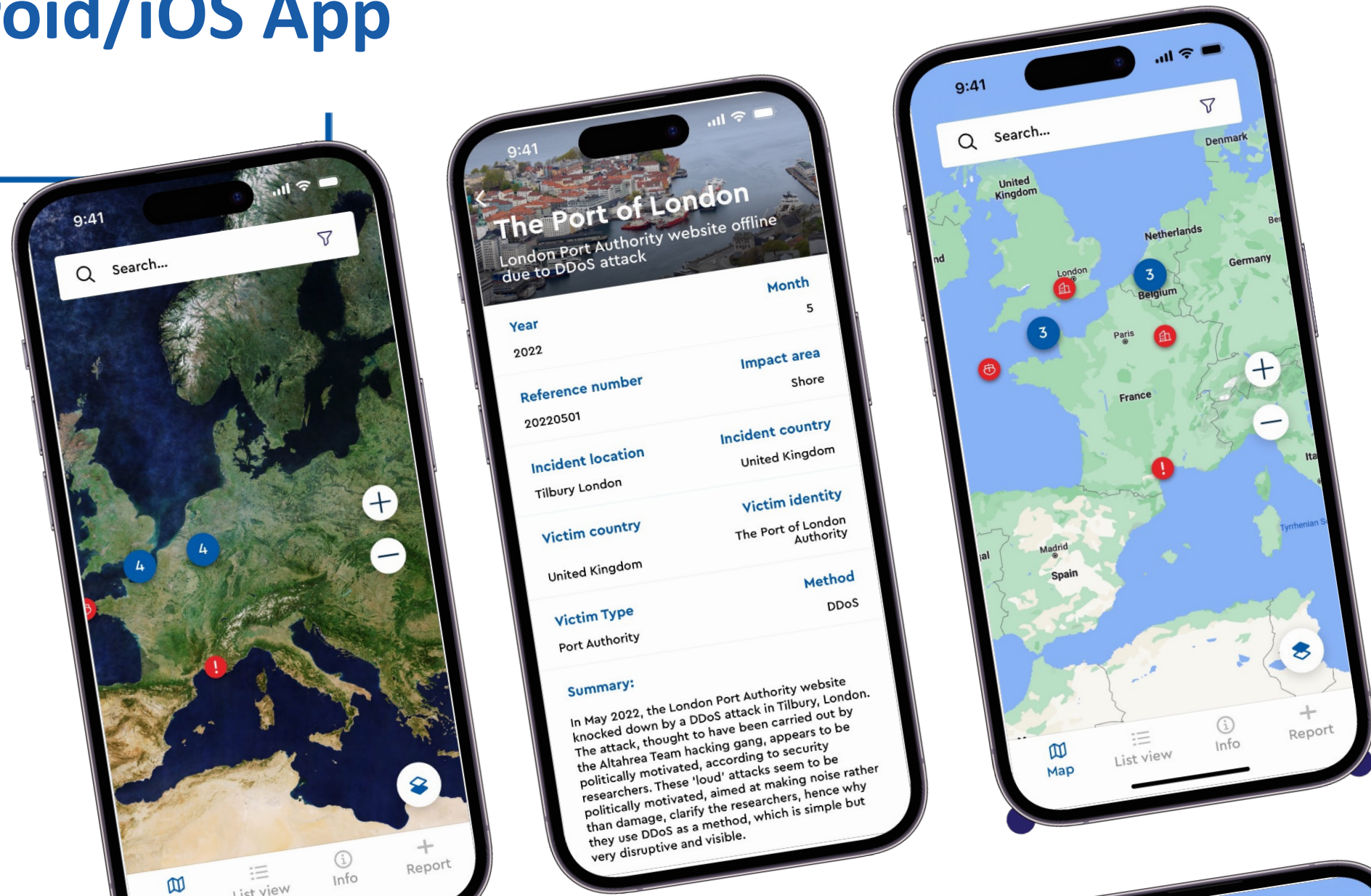
Maritime Cyber Incidents 2001-2021



Database of Maritime Cyber Incidents

- Already over 150 Maritime Cyber Security Incidents identified (2001 to 2022)
- Previous research in 2020, “A Retrospective Analysis of Maritime Cyber Security Incidents” (Meland et al) only identified 46
- Over 50 involving vessels, 39 on shipping companies, 38 used ransomware (all since 2018) and 22 on ports
- Impacts on IT, OT, Network, Navigation (ECDIS/GPS/AIS) and numerous others systems
- Incident attribution includes numerous known nation state and criminal threat actor groups (Top source countries: Russia, China, Iran, North Korea)

Android/iOS App





USS Harry S Truman

- In 2014 a US Nuclear Aircraft Carrier was subject of an investigation into hacking of numerous computer systems including systems belonging to the US Navy and US Geospatial-Intelligence Agency
- NCIS agents tracked down a suspect and conducted an investigation on board after transferred to the ship at sea by aircraft





The Hacker

- The suspect was Nicholas Paul Knight and he was a member of hacking group “tEam Digi7al”
- He was also an IT systems administrator on board the Harry S Truman
- His job was running the network in the nuclear reactor department
- NCIS set a fake database server which he breached and he was arrested
- Sentenced to 2 years jail

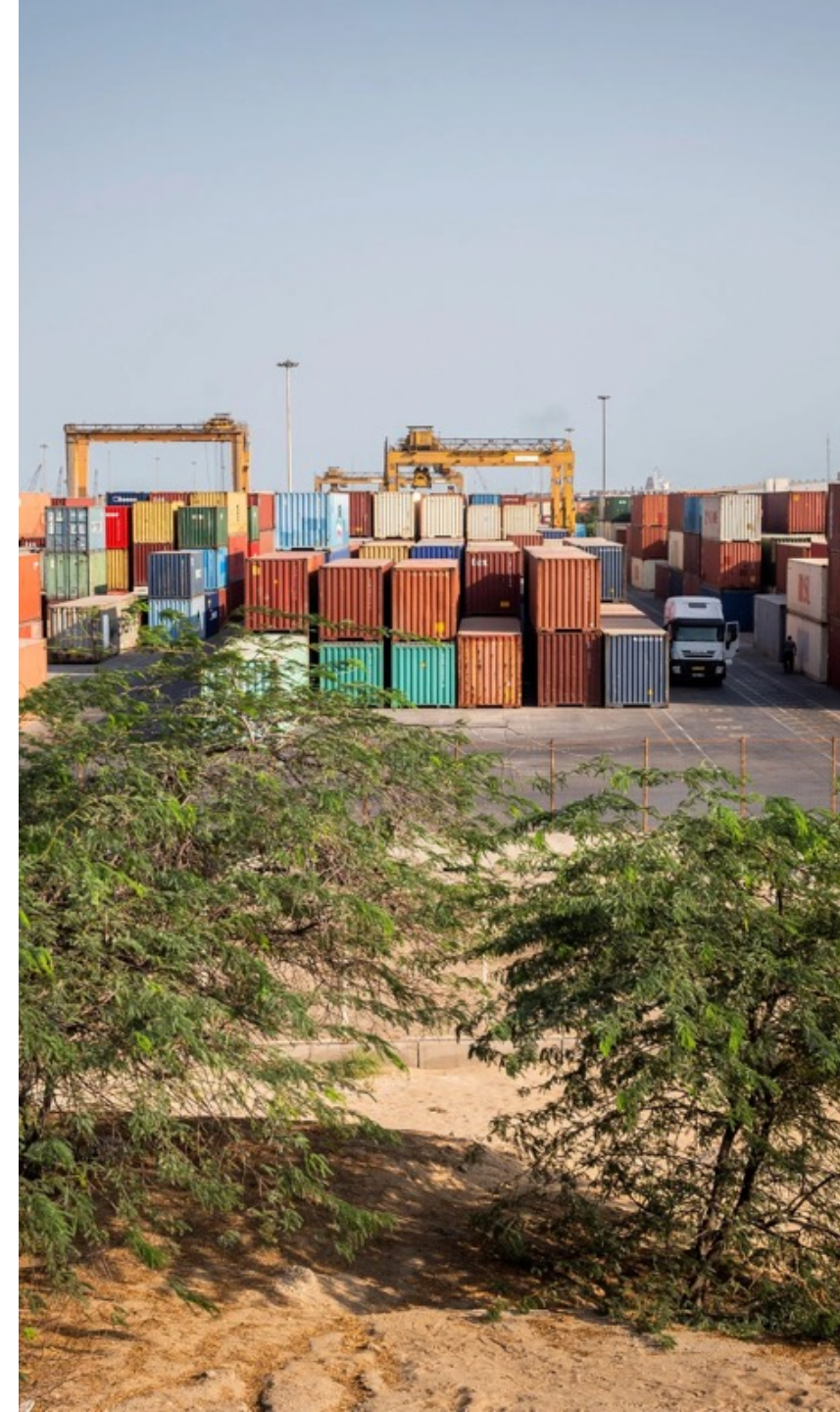


GPS Jamming 2016 (BBC News 2016)

- In 2016 North Korea was suspected of jamming GPS signals in South Korea
- North Korea is using radio waves to jam GPS navigation systems near the border regions, South Korean officials claimed
- The broadcasts have reportedly affected 110 planes and ships and can caused mobile phones to malfunction
- The South Korean coastguard reported about 70 fishing vessels had been forced to return to port after GPS navigation issues

Israel/Iran Cyber Conflict (NYT)

- In May 2020 Israel was behind a cyberattack that disrupted a major port in Iran, Shahid Rajaee, done in response to an attempt by the Revolutionary Guards to infiltrate an Israeli water facility
- Soon after the cyberattack began, the port's authorities detected it but failed to fix it immediately so switched to manual management of unloading and loading
- The chief of staff of the Israel Defense Forces, said, "We will continue to use a diverse array of military tools and unique warfare methods to hurt the enemy"
- In a deadly escalation in July 2020 an oil tanker managed by an Israeli-owned shipping firm was attacked by drones off the coast of Oman, killing two crew members
- "The pattern of the attack and the outcome seems like a serious escalation in the Iranian-Israeli 'tit for tat' engagement that has been ongoing in the maritime domain over the last couple of years"



Hackers breached computer network at key US port but did not disrupt operations



By [Sean Lyngaas](#), CNN

Updated 2235 GMT (0635 HKT) September 23, 2021



A container is shown being transported at the Port of Houston on July 29, 2021, in Houston, Texas.

(CNN) — Suspected foreign government-backed hackers last month breached a computer network at one of the largest ports on the US Gulf Coast, but early detection of the incident meant the intruders weren't in a position to disrupt shipping operations, according to a Coast Guard analysis of the incident obtained by CNN and a public statement from a senior US cybersecurity official.

NEWS & BUZZ



CNN reporter says Steve Bannon's admission creates a 'huge...'



Saving money using cryptocurrency swaps



Maritime Supply Chain Attack (maritime-executive.com Nov 2021)

- Danaos Management Consultants has been offering IT solutions for the maritime industry since 1986
- It builds software tools for ship management, including applications for chartering, payroll, crewing, AI analytics, ISM, document management and procurement
- The ransomware attack blocked customers communication with ships, suppliers, agents, charterers and supplies, while at the same time the files with their correspondence were lost.
- It has been reported that Danaos maintained open VPN links with customers and vessels

Cyberattack Hits Multiple Greek Shipping Firms



Port of Piraeus, the center of Greek shipping (File image courtesy Jeffrey / CC BY ND 2.0)

PUBLISHED NOV 3, 2021 7:50 PM BY **THE MARITIME EXECUTIVE**

Multiple Greek shipping companies have been hit by a ransomware attack that spread through the systems of a popular, well-established IT consulting firm, according to Greek outlet Mononews.

Danaos Management Consultants, the IT service provider whose services were affected by the hack, confirmed the incident and. The company said that Danaos' own shipping operations have not been hit, and that fewer than 10 percent of its external customers had their files encrypted by the ransomware attack.

An independent cybersecurity company has been contracted to investigate the incident and determine how the ransomware got inside Danaos' customer-facing systems. Meanwhile, the firm is helping affected clients as they try to restore their systems.

Coastguards are even a target (2004 & 2014)

W News ▶ Latest Wales News

Coastguard hit by bug

COASTGUARDS around the UK were yesterday hit by an internet bug which caused computers to crash.

NEWS By WalesOnline

00:00, 5 MAY 2004 | UPDATED 18:19, 31 MAR 2013

Bookmark



▶ Enter your **postcode** for **local news** and **info**

Enter your postcode

Go

In YourArea

COASTGUARDS around the UK were yesterday hit by an internet bug which caused computers to crash.

Staff reverted to using pen and paper until early afternoon after the system was damaged by the Sasser virus.

Sponsored Link by Taboola



Maritime Denmark



Follow

News ▾ Magazines ▾ Careers ▾ Newsletter ▾ Advertising ▾ Contact Us ▾ RSS Danish
Home Shipping Industry Services Offshore Ports Short News New ships Off-duty Video Pictures Events

The DMA attacked by hackers



22-09-2014 16:00:00



TV news could reveal Sunday night that hackers from a foreign state in the spring of 2012 made their way to the Danish Maritime Authority IT systems in search of confidential information. Government IT, Business, and Growth Ministry were also attacked.

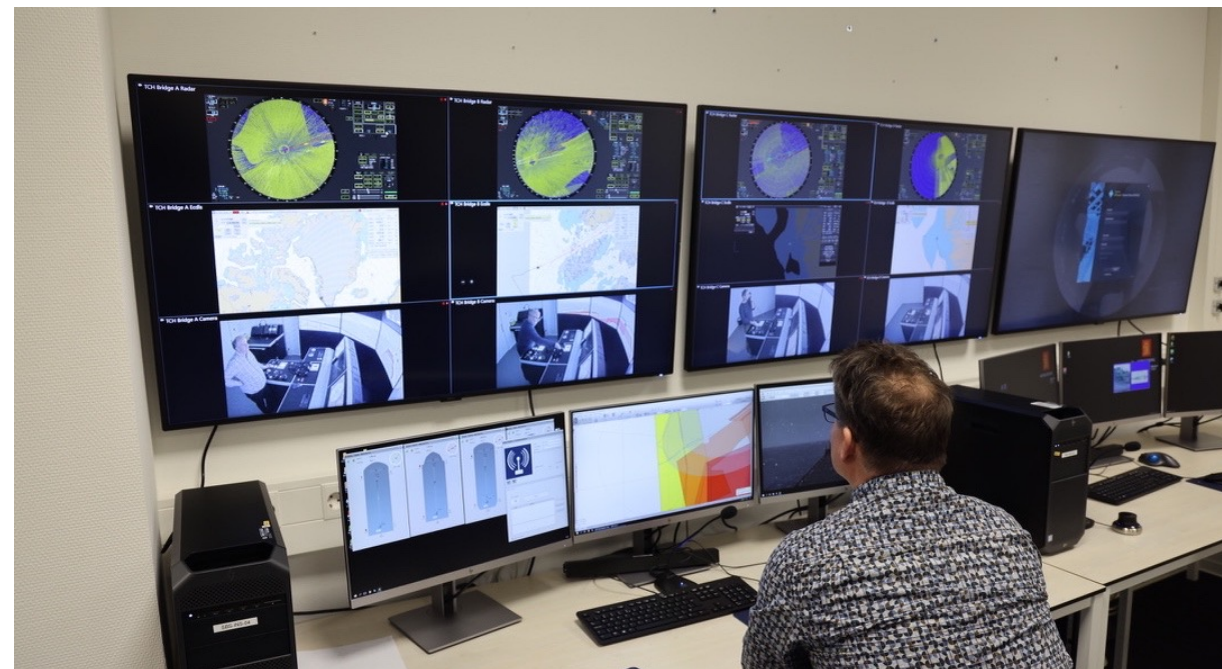
DR News had access to previously confidential reports, which states that "the attack was state-sponsored and very professionally done." Reports will not disclose which country was behind the attack, but according to DR information points suspicion against China.

The Chinese Embassy denies any knowledge about the attack.



Maritime Cyber Incident Simulations

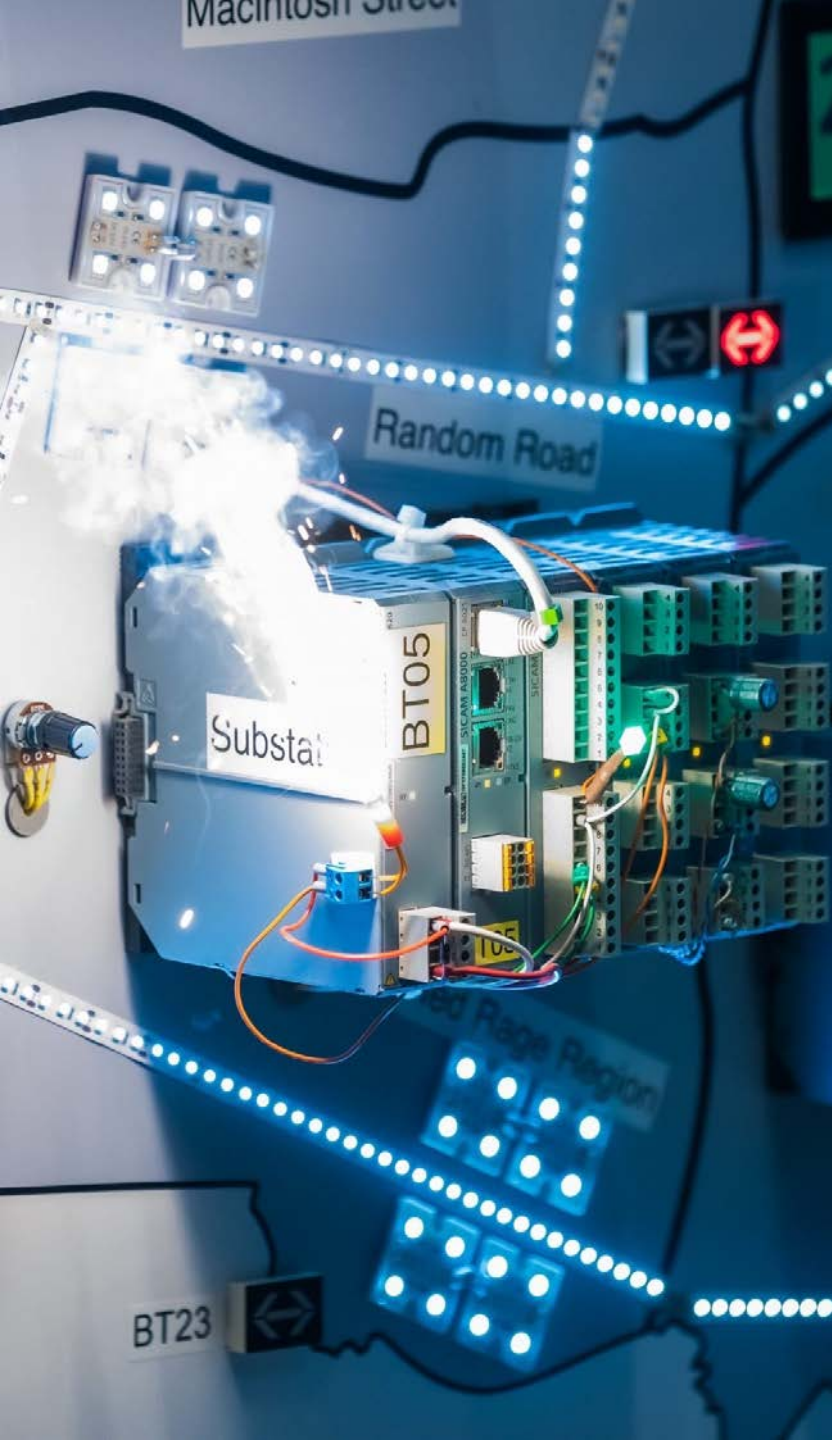
- Maritime Cyber Incident simulations will be developed to enhance security awareness, train participants in correct response procedures and study human factors in these types of scenarios.
- These simulations will include:
 - Crew simulations using facilities at the Maritime Institute on Terschelling
 - Software simulation based on existing work by Serious Gaming
 - Tabletop exercises for executives, conferences, etc.
 - Large scale exercises utilising a combination of the above across multiple sites



Threat	Deviation of electronic position due to cyberattack on ECDIS/GPS
Materials used	• Introduction exercise • Simulator • Ship model CNTRN43.B • Deviation of electronic position • Flowchart/Game Martin • Research/observation form • Evaluation form
Scenario research questions	Observations: (What do we want to investigate and why?) The effect of actions in whether or not to register deviation to navigation equipment such as the ECDIS. Research questions: - How long did it take until an anomaly was detected - What is the primary reaction to this anomaly? - What is the secondary response to this anomaly? - Is there awareness that equipment may have been hacked? - How does this awareness come about - If there is awareness that the equipment is infected with a virus what is the primary response? - What is the secondary response?





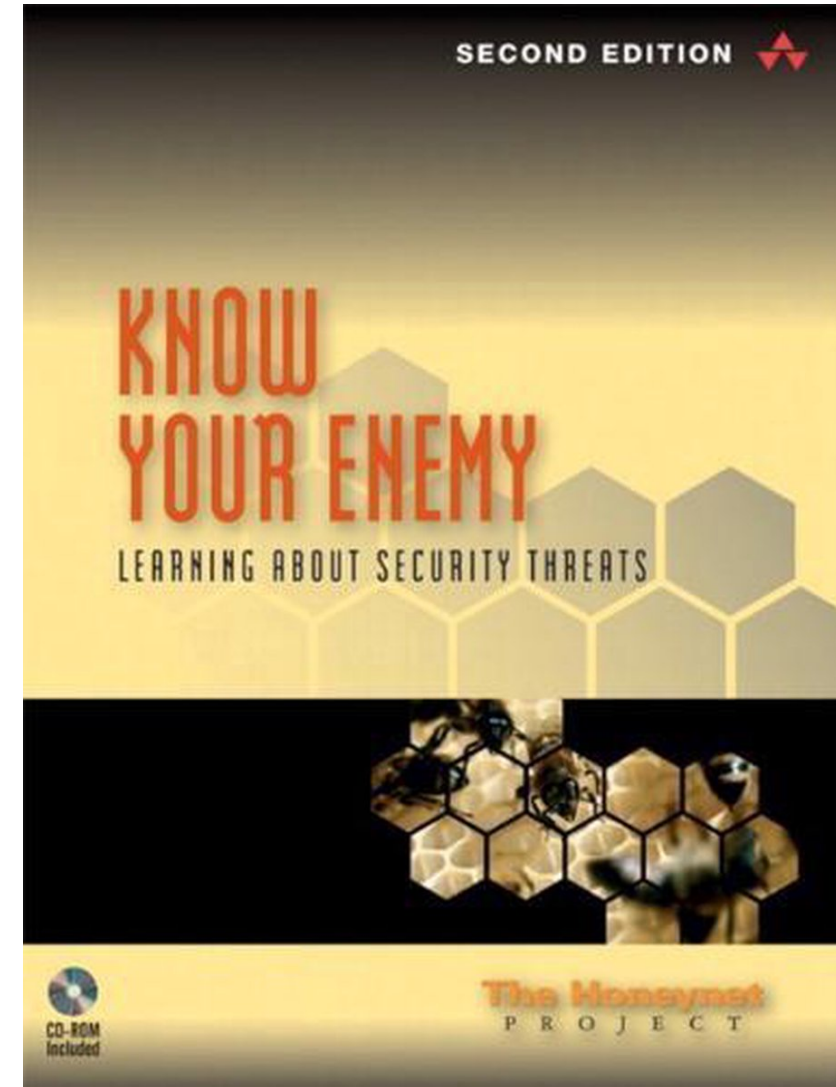


Create Maritime Technology Hacking Lab

- Build lab environment utilising equipment from maritime industry technology providers
- Based on known issues from other ICS/SCADA industries and maritime conduct vulnerability research in lab environment
- Build a virtual ship Honeynet to study current active scanning of maritime technology
- Use discovered vulnerabilities and Honeynet data to develop:
 - Research reports/publications
 - Report vulnerabilities
 - Utilise in maritime cyber incident simulations

Maritime Honeypot

- A honeynet is a network set up with intentional vulnerabilities hosted on a decoy server to attract hackers
- So a honeynet consists of one or more honeypots





TOTAL RESULTS

15

TOP COUNTRIES



Cambodia	12
Cyprus	1
Hong Kong	1
Norway	1

TOP PORTS

53	9
1723	2
25	1
135	1
8081	1

More...

TOP ORGANIZATIONS

SOUTH EAST ASIA TELECOM (Cambodia) Co., LTD	8
Starchain Telecom Co., LTD.	2
Flat 13, 4/F Trans Asia Ctr	1
Hellas Sat Consortium Ltd	1
MekongNet Nationwide Network Coverage	1

 View Report  View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

213.234.126.3 ↗

Telenor Satellite AS

 Norway, Skålevik

HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Cache-Control: must-revalidate = no-cache
Content-Type: text/html

```
<!DOCTYPE html>
<html>
<head>
<!--
***** index.html *****
main page frame for Seatel/Cobham
author: Michael Ryan
copyright: 2014
--...

```

2022-06-16T10:59:22.142682

103.230.228.230

Flat 13, 4/F Trans Asia Ctr

 Hong Kong, Tsuen Wan

why query me?
Recursion: enabled
Resolver name: SEATEL-CACHE-1

2022-06-16T05:18:08.768807

94.125.145.70 ↗

Hellas Sat Consortium Ltd

 Cyprus, Nicosia

HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Cache-Control: must-revalidate = no-cache
Content-Type: text/html

```
<!DOCTYPE html>
<html>
<head>
<!--
***** index.html *****
main page frame for Seatel/Cobham
author: Michael Ryan
copyright: 2014

```

2022-06-16T00:34:15.668030

Screenshot

Sea Tel

COBHAM

Login Id

Password

Submit

Cancel



Sat Lon:
Heading: 0
Azimuth: 0
Elevation: 0
Relative: 0
Lpolang: undefined

Signal



Track

On

Off

Wizard

Commission

Configuration

Interfaces

System

Reflector

Status

Graphs

System

Tools

CLI Command

Position Antenna

Test

Logs

Activity

Data Export

Others

Admin

Help

System Status

System

● Modem Rx Lock: LOCKED
● Tx Mute: OFF
● Error: ERRORS
Search Delay: 30 seconds
Sat Reference: ON(ACTIVE)

Satellite

Name: CUSTOM
Position: 53.0 W degree
Frequency: 1126.6
Search Pattern: SKY SEARCH
Auto Threshold 100
Offset:
Threshold: 1541

Front Panel Led

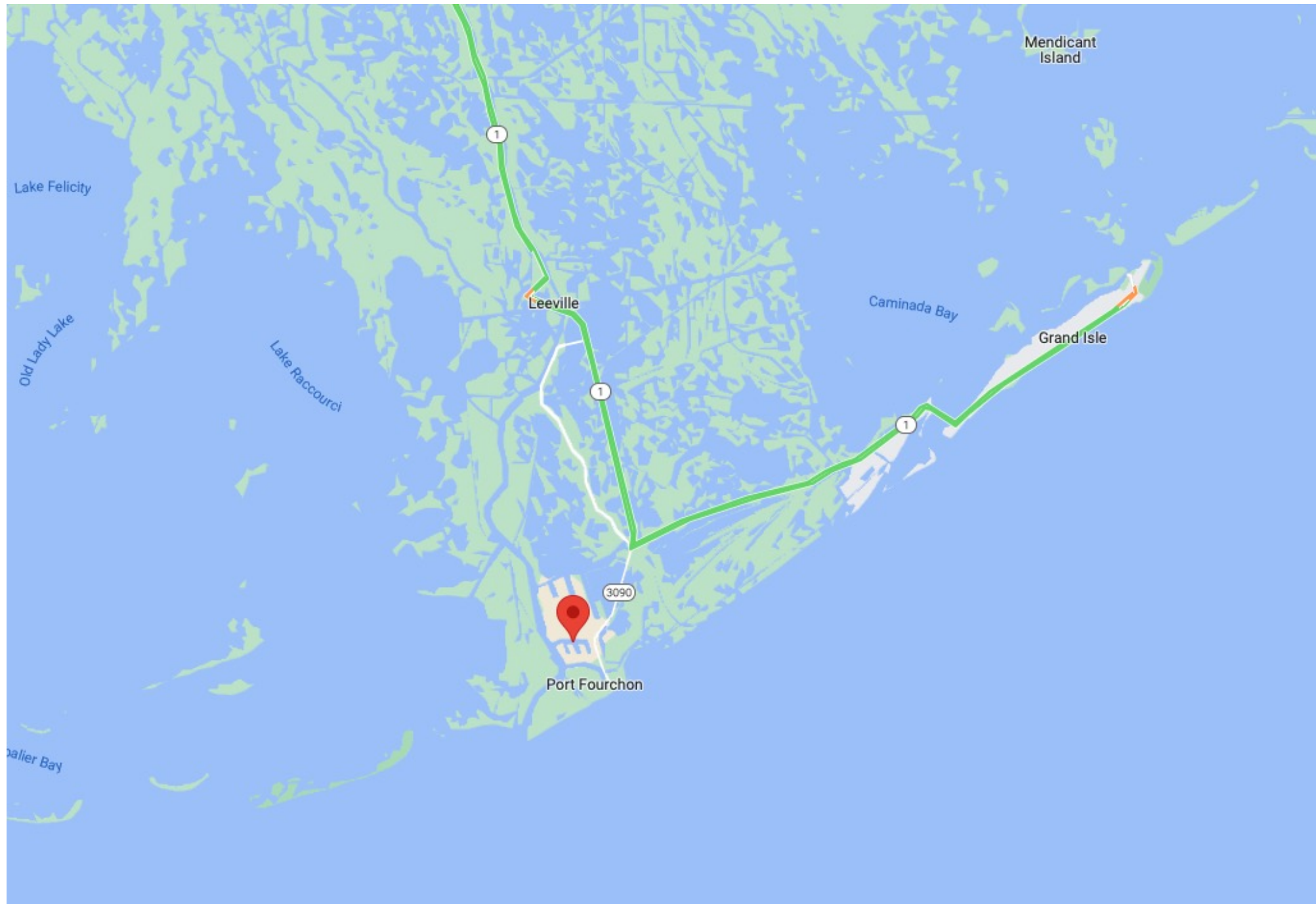
Modem: GMXP:
● Net ● Power
● Tx ● Status
● Rx1
● Rx2 ● ADU power
● Status ● CM power

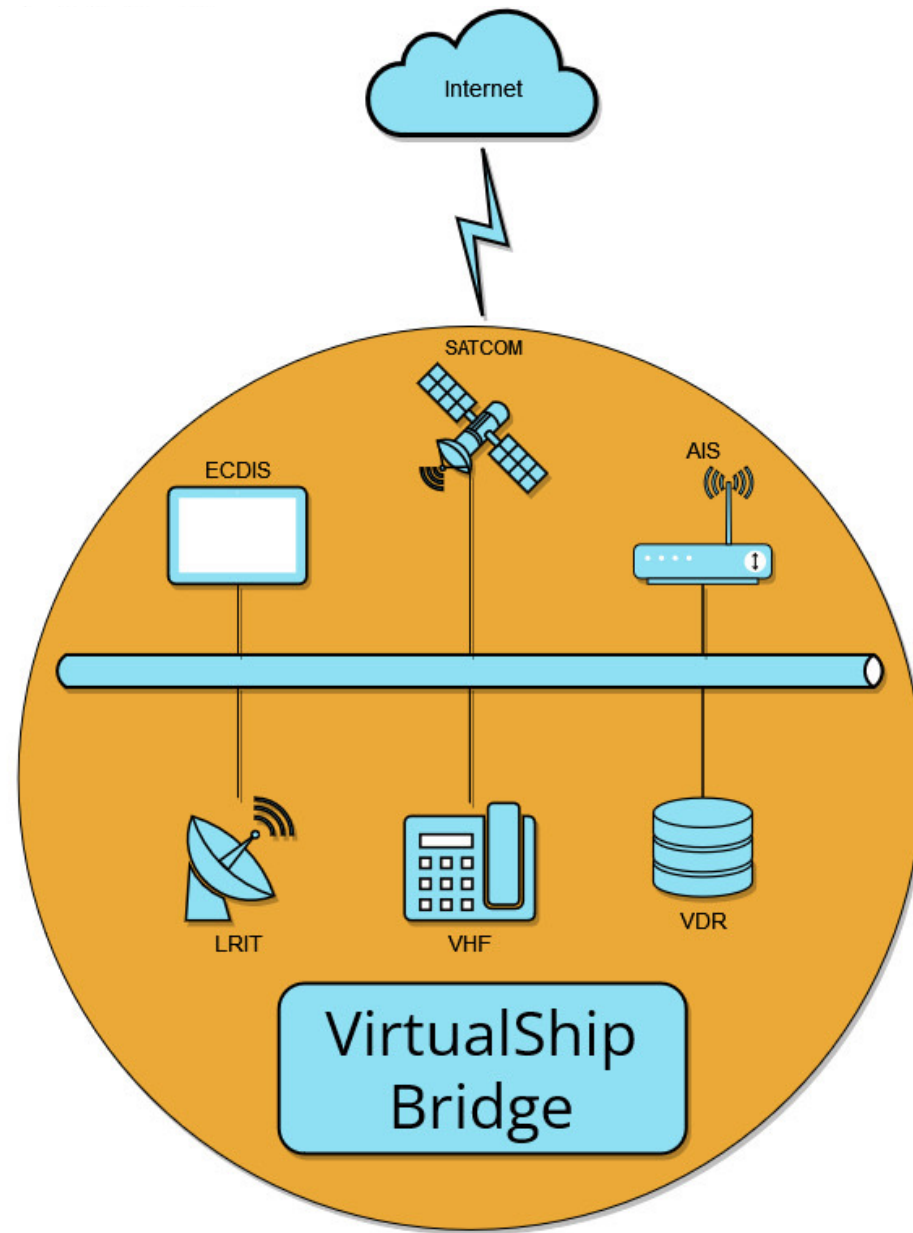
Ship

Latitude: 29.121323 N degree
Longitude: 90.203781 W degree

Antenna

Cross Level: -0.0 degree





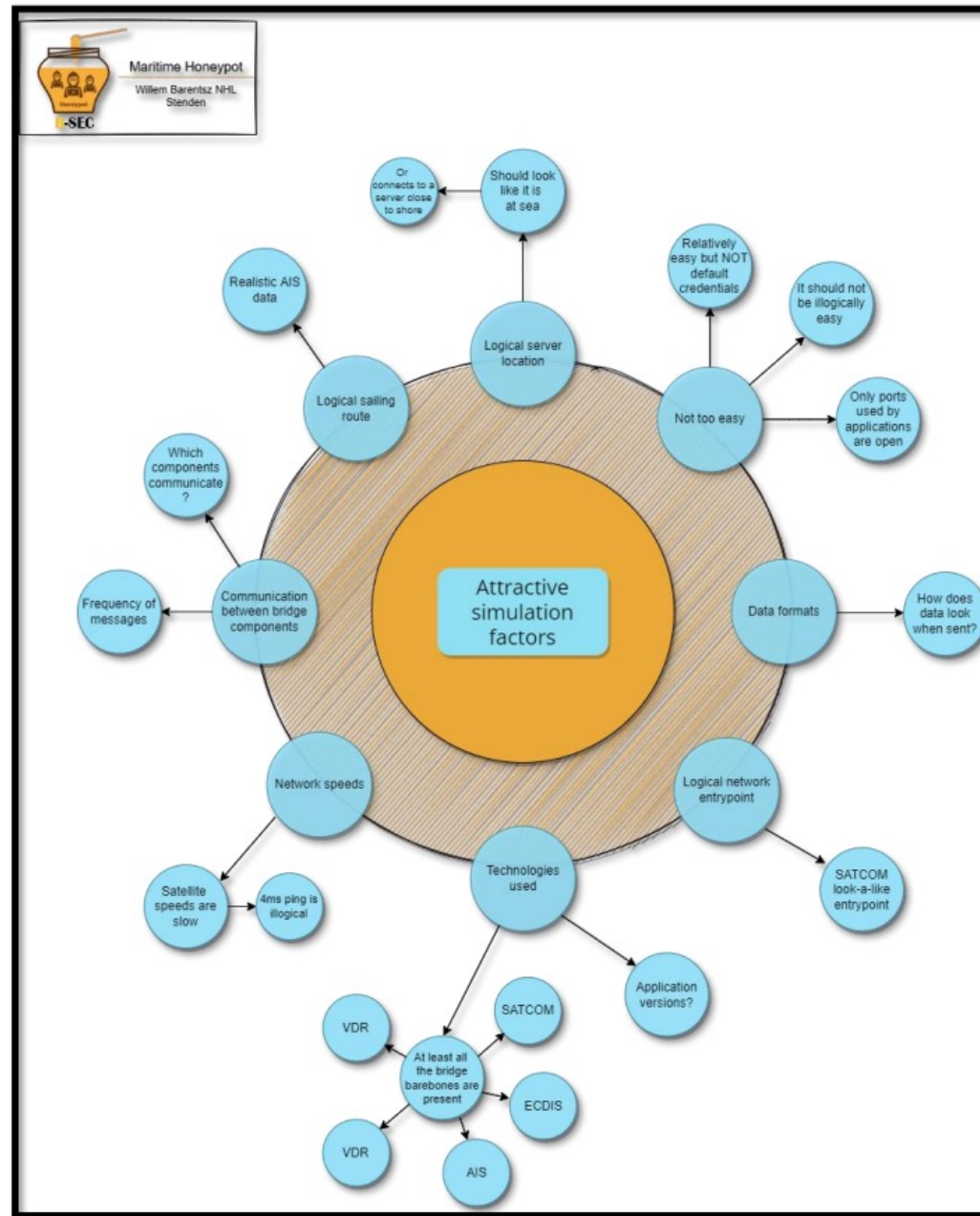


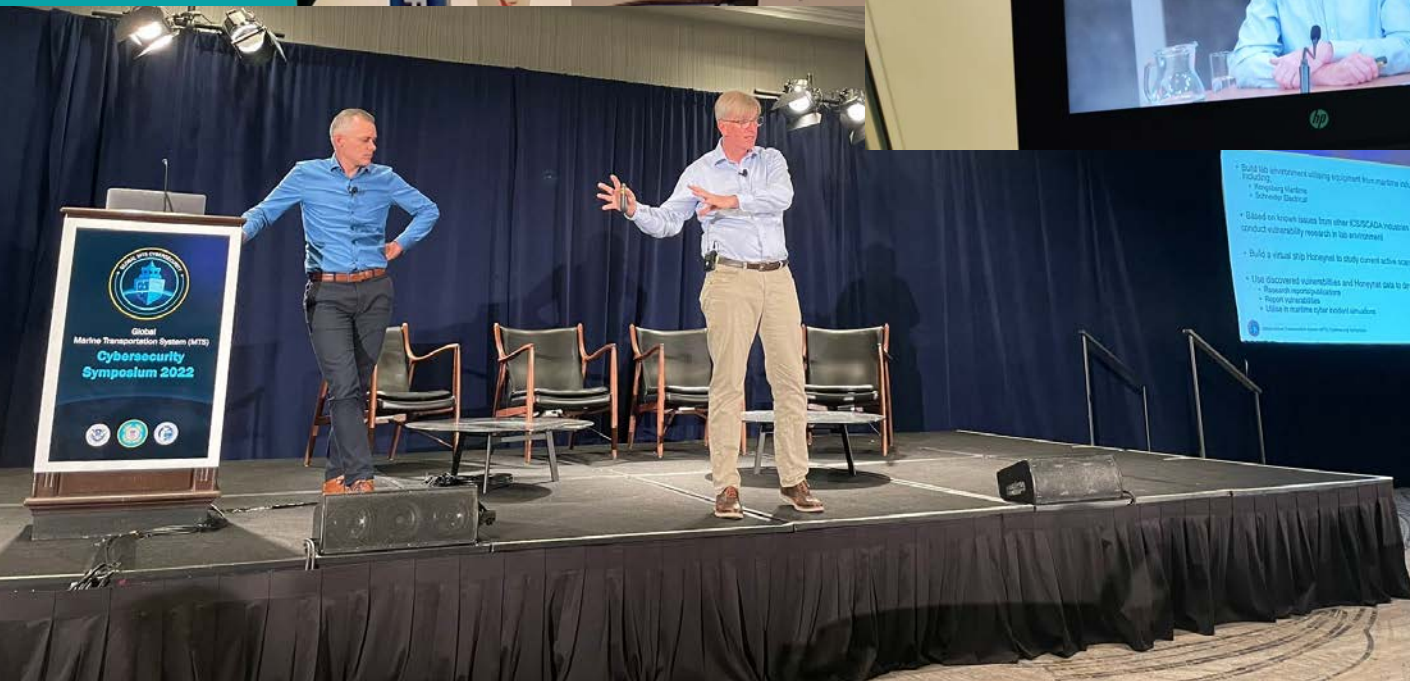
Figure 4 – Mindmap attractive simulation factors.

Current Cyber Threats to Maritime Security

Webinar – 13th April 2022

NHL
STENDEN
university of
applied sciences

NHL
STENDEN
hogeschool



- Build the environment using equipment from maritime industry
- Research Marine
- Software Design
- Based on known issues from other EUSCADA regions and conduct vulnerability research in the environment
- Build a virtual ship horizon to study current active warning
- Use discovered vulnerabilities and Horizon data to develop
- Research report generation
- Report vulnerabilities
- Use in maritime cyber incident simulation



OTV
News Flash

Port of Orangeland Cyber-attack

Questions



university of
applied sciences