

Maritime IT Security Research Group

Stephen McCombie



university of
applied sciences



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

CARBON CO₂ 154,712 t

FREIGHT Containers 14,737,118 Dry 579,195 kt Liquids 420,788 kt Gas 63,241,080 m³ Vehicles 10,507,073 kt

OPTIONS Show Colours Filters



16 November 2012 07:00



Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

Global Maritime Transportation System

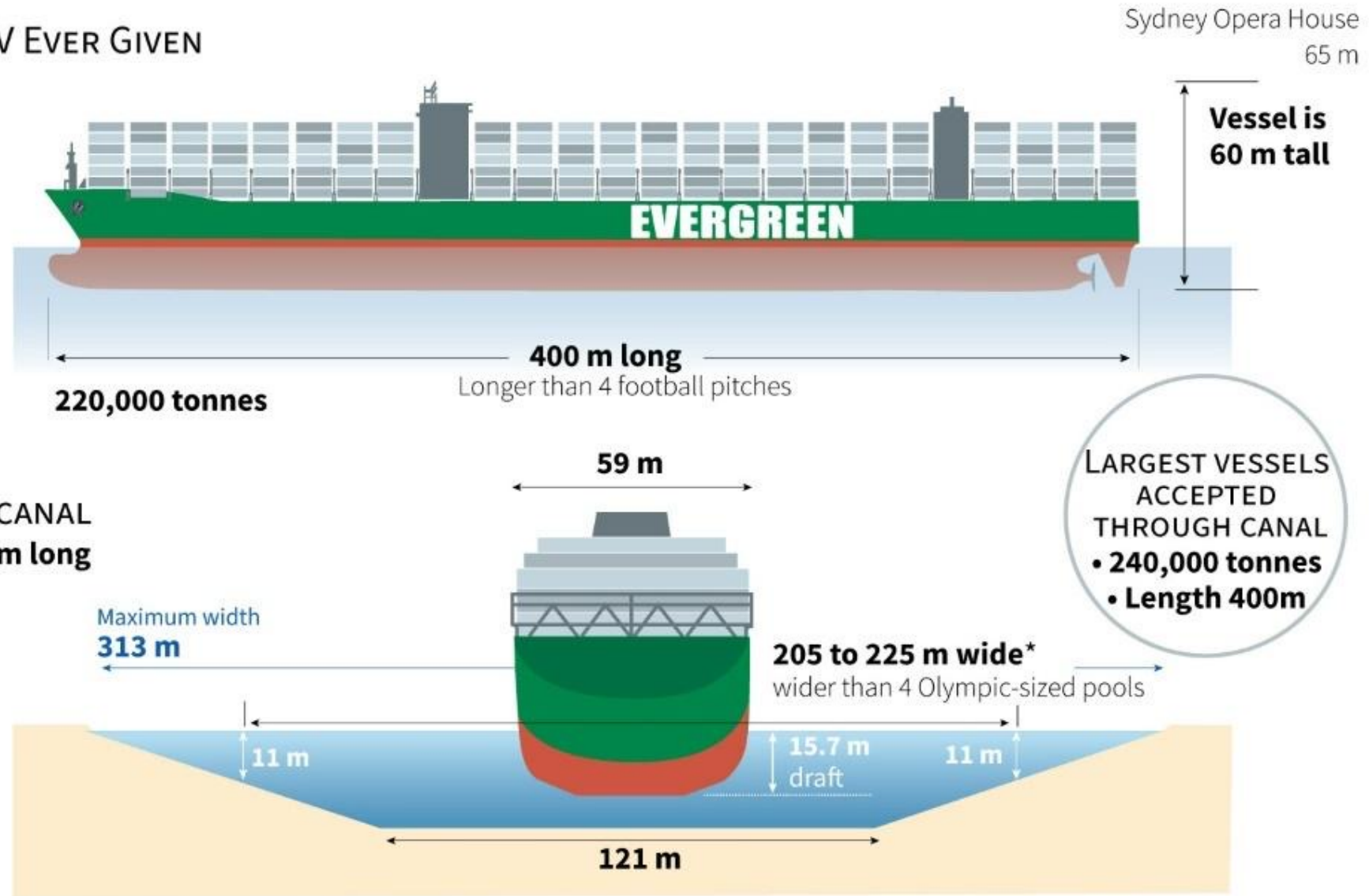
- The role of GMTS in the global economy is significant with over 80% of the world's cargo transported by ship (Bronk & Dewitt 2020) and representing 70% of global trade by value (Loomis & Singh, et al 2021).
- At the same fleets are aging and their technology is aging with them and thus more vulnerable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



MV Ever Given and the Suez Canal

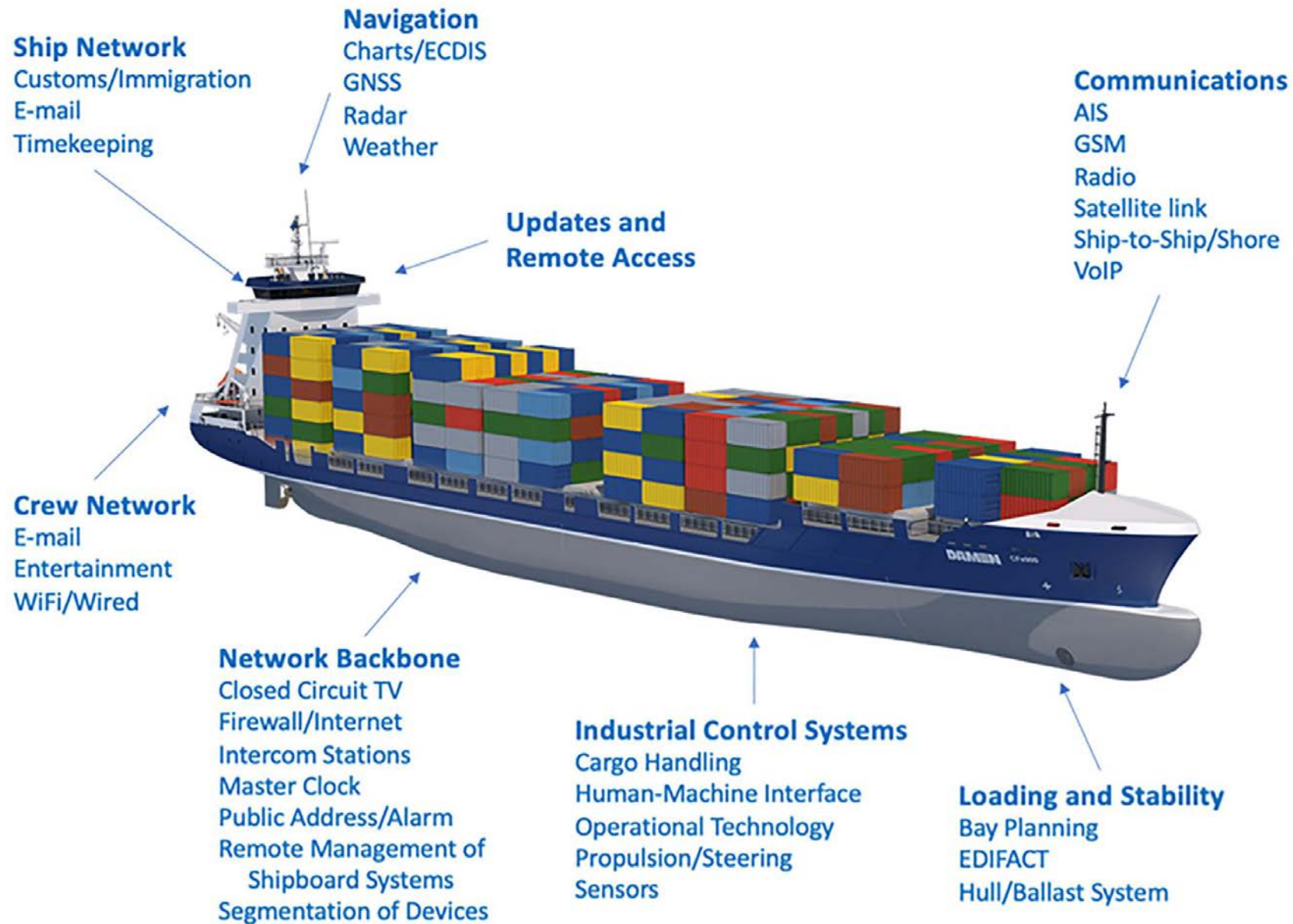
The huge container ship of the Evergreen Marine Corporation has blocked the canal

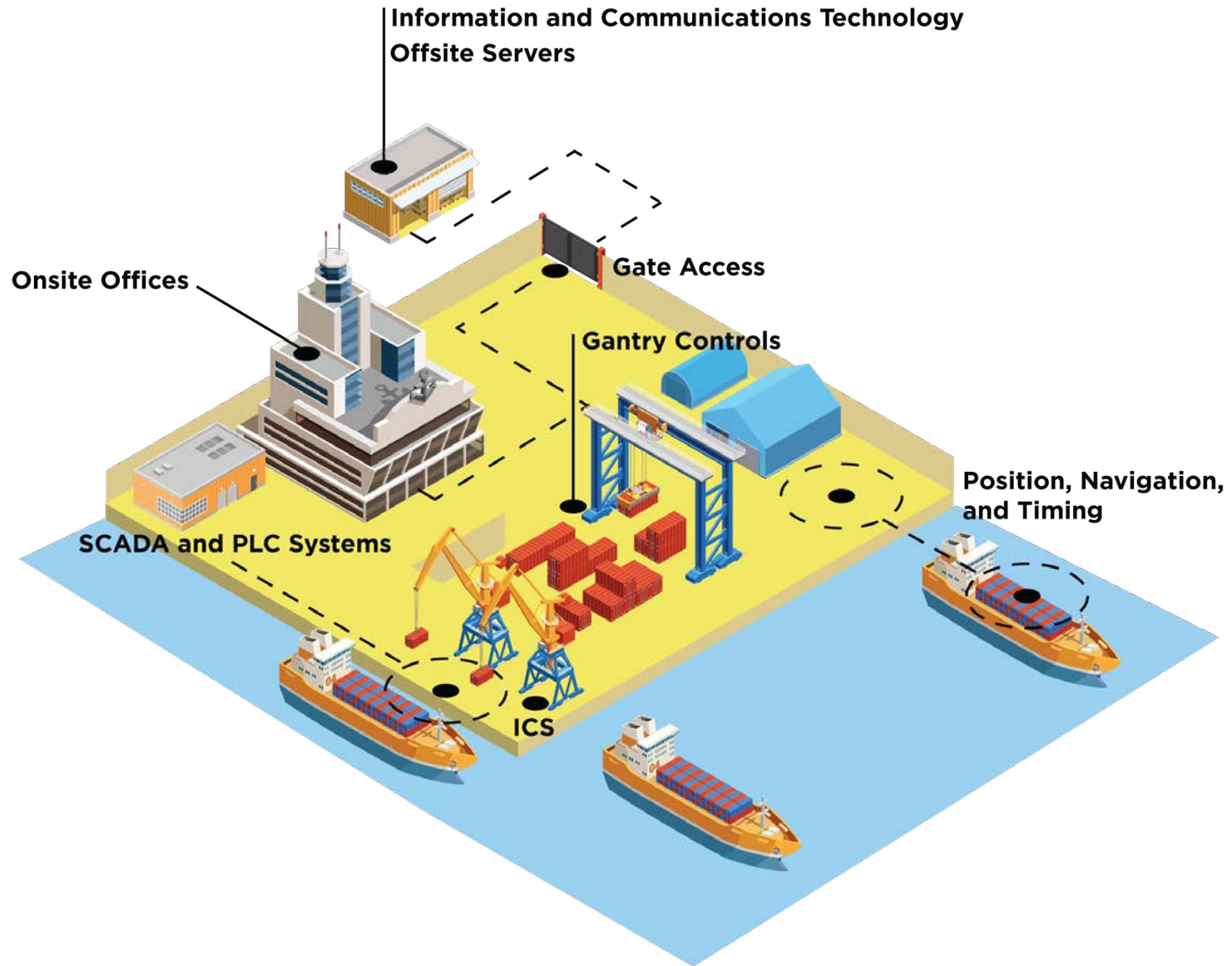
THE MV EVER GIVEN





(Kessler and Shepard 2022)





Why is the maritime industry so vulnerable?



- Poorly maintained and aging equipment
- Low level of cyber security maturity and awareness
- Lack of cyber security staff
- Potentially serious safety issues as a result of cyber attacks
- Critical nature of Maritime Sector for global economy and security
- Various threat actors targeting it

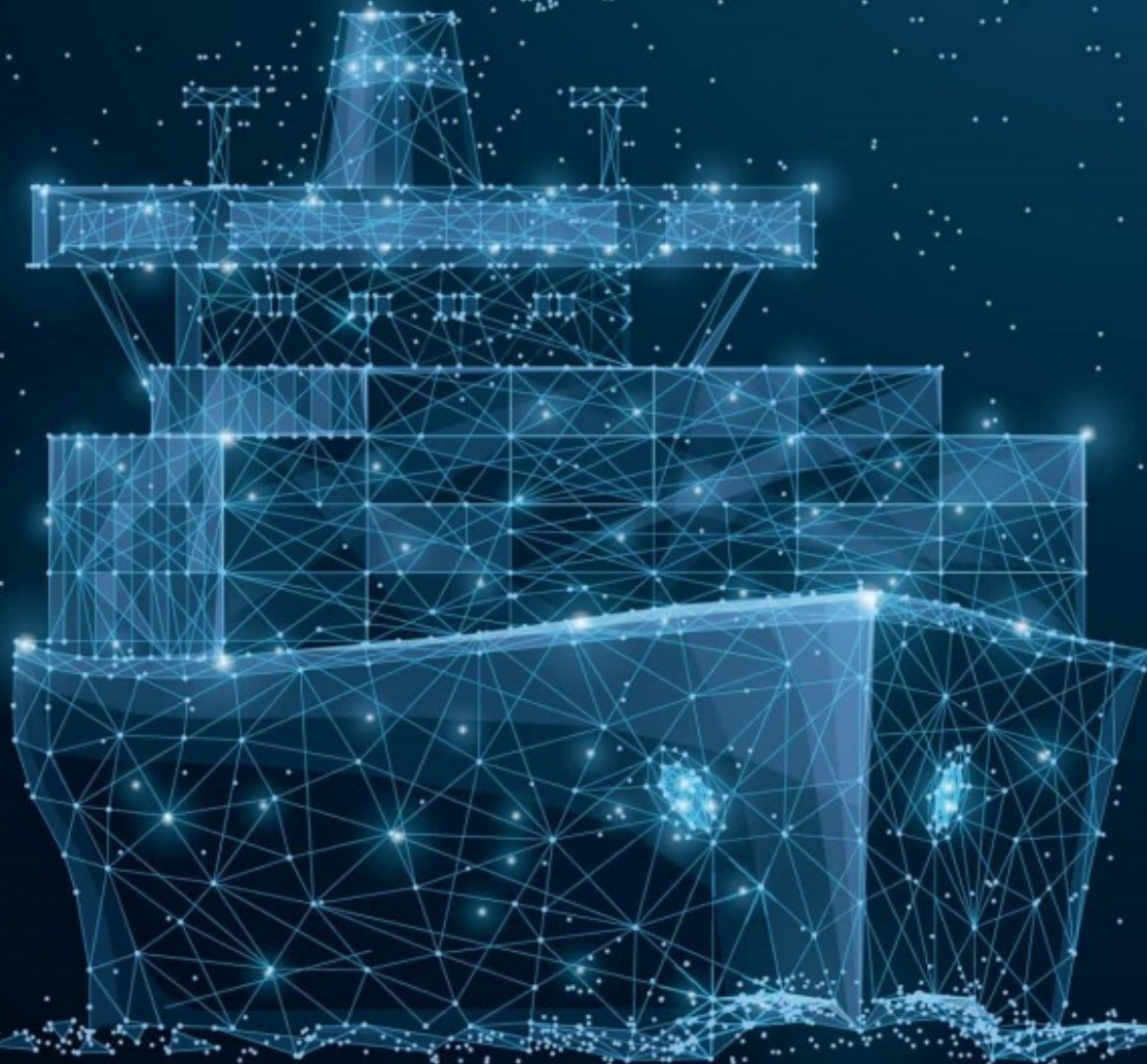




Database of Maritime Cyber Incidents

- 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.



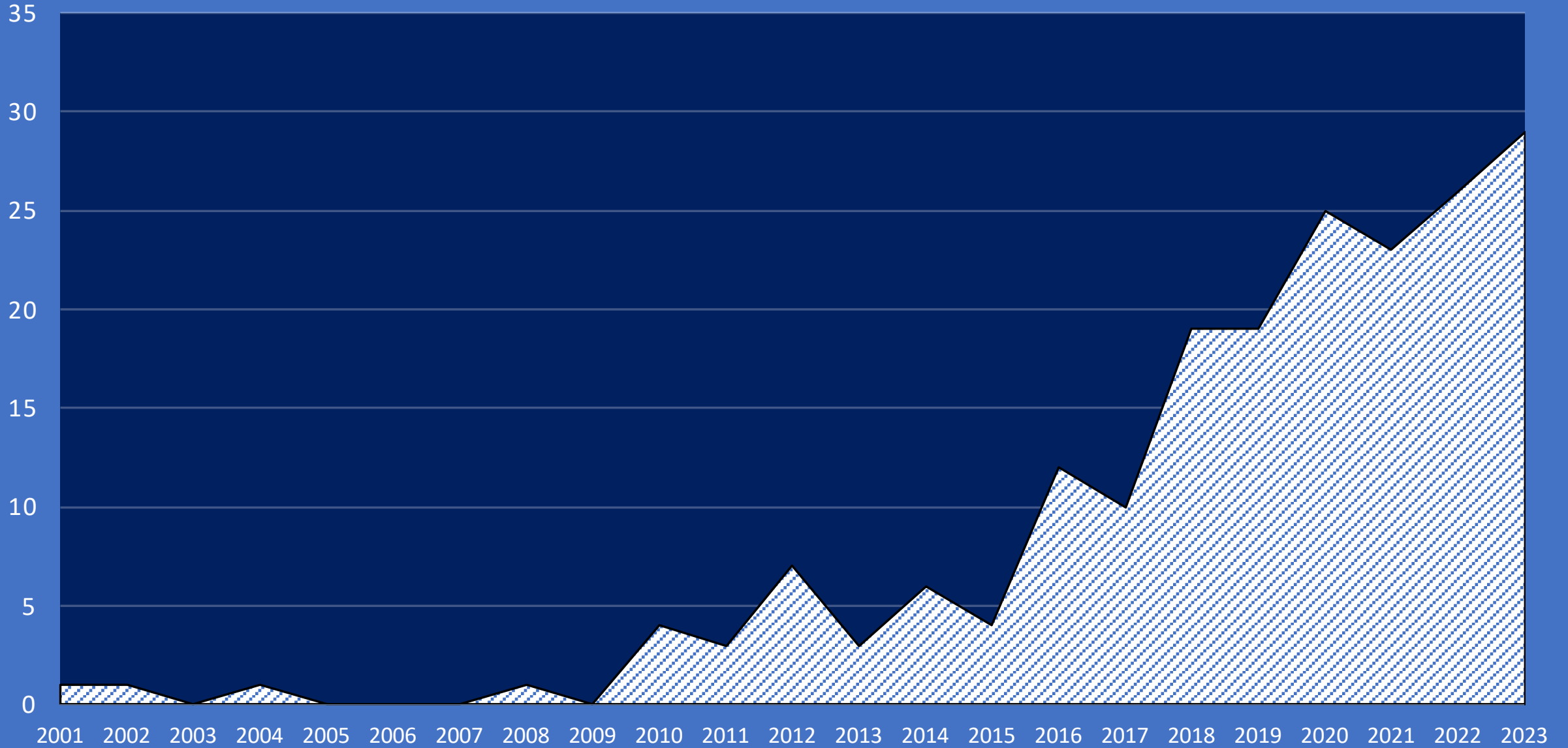


STIX Database

The place for maritime cyber incidents reporting

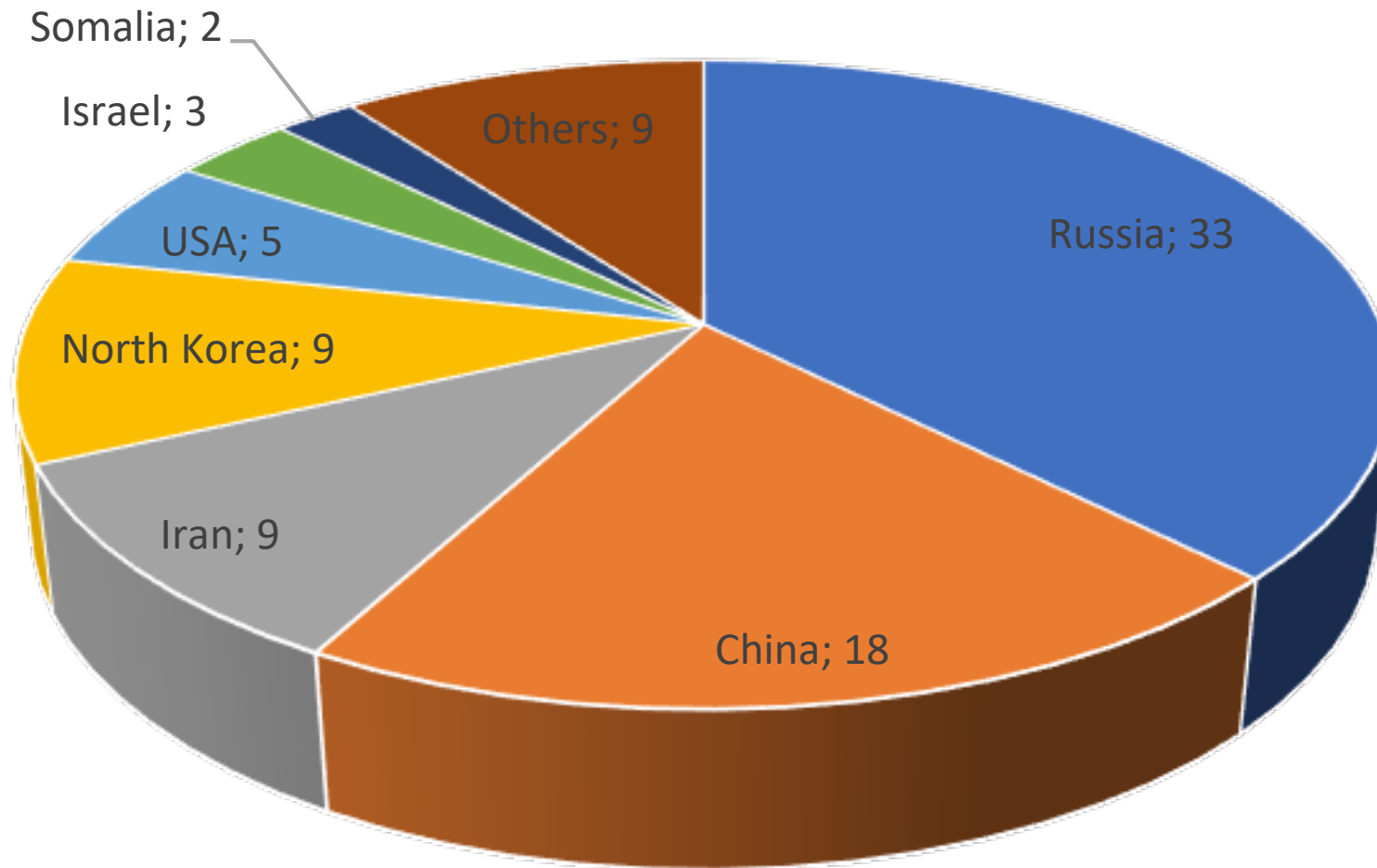
[Login/Register](#)

Martime Cyber Incidents by Year 2001-2023



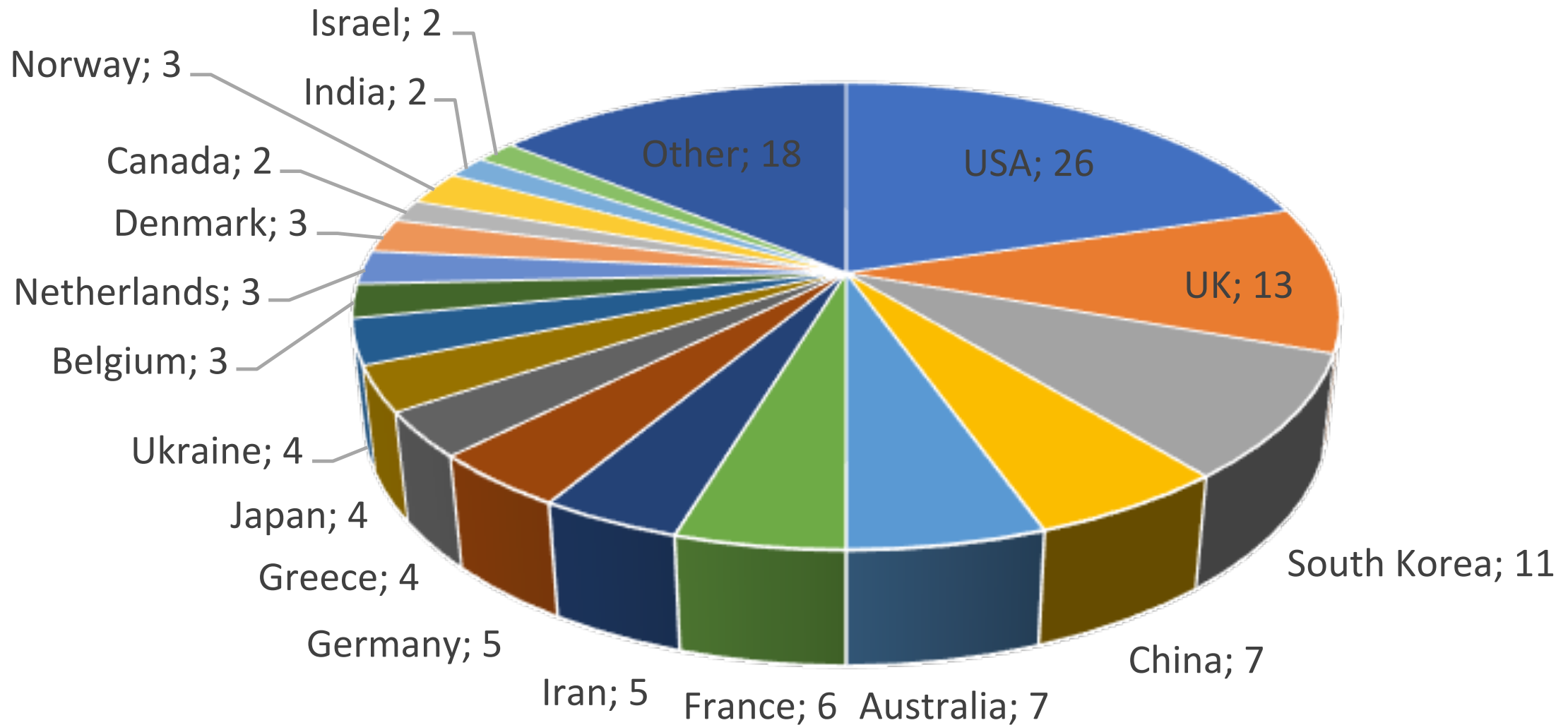


Cyber Incidents by Attacker Country 2001-2022

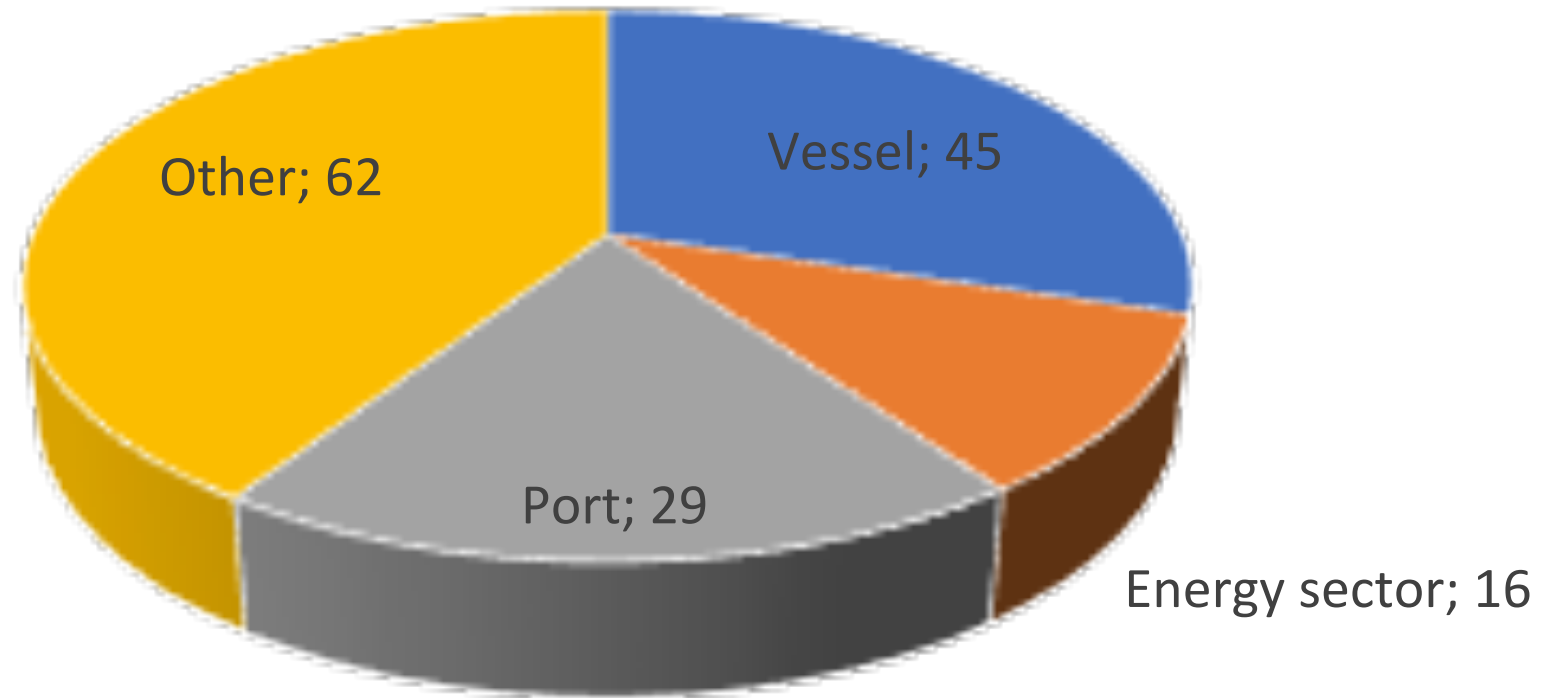


■ Russia ■ China ■ Iran ■ North Korea ■ USA ■ Israel ■ Somalia ■ Others

Maritime Cyber Incidents by Victim Country 2001-2022



Maritime Cyber Incidents by Victim Type 2001-2022

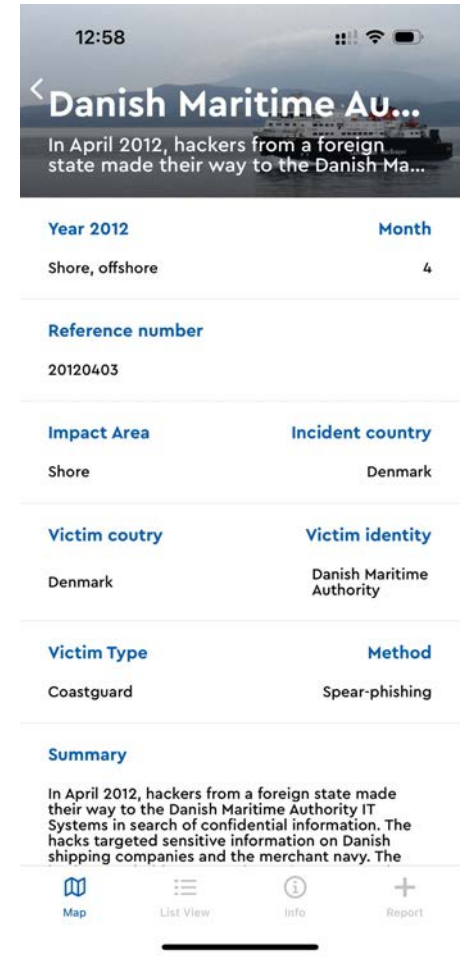
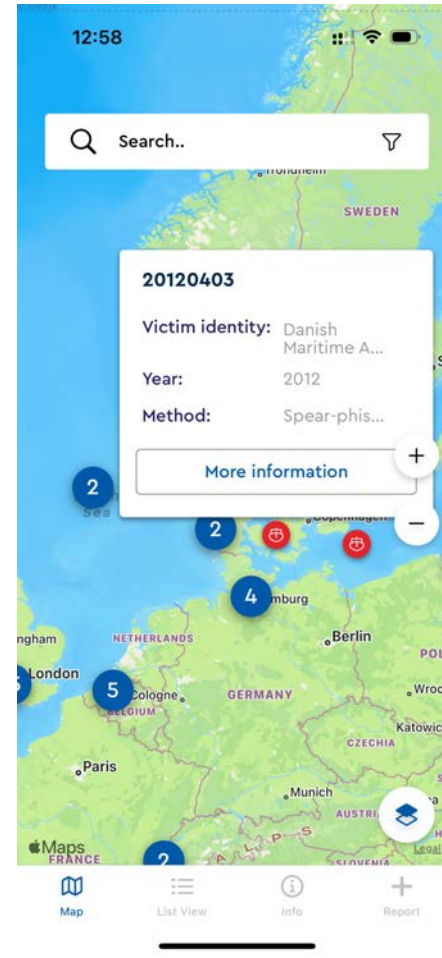
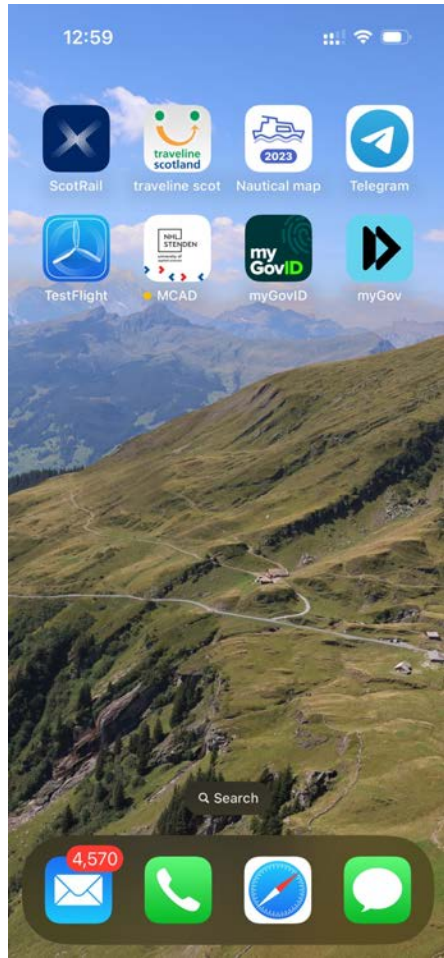


■ Vessel ■ Energy sector ■ Port ■ Other

Search in the map... 🔍



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 cause mobile phones to malfunction
- The South Korean coastguard reported about 70 fishing vessels had been forced to return to port after GPS navigation issues

GPSJam

Daily maps of GPS interference
[About](#) | [FAQ](#)

25/05/2023

More

Atlantic Ocean

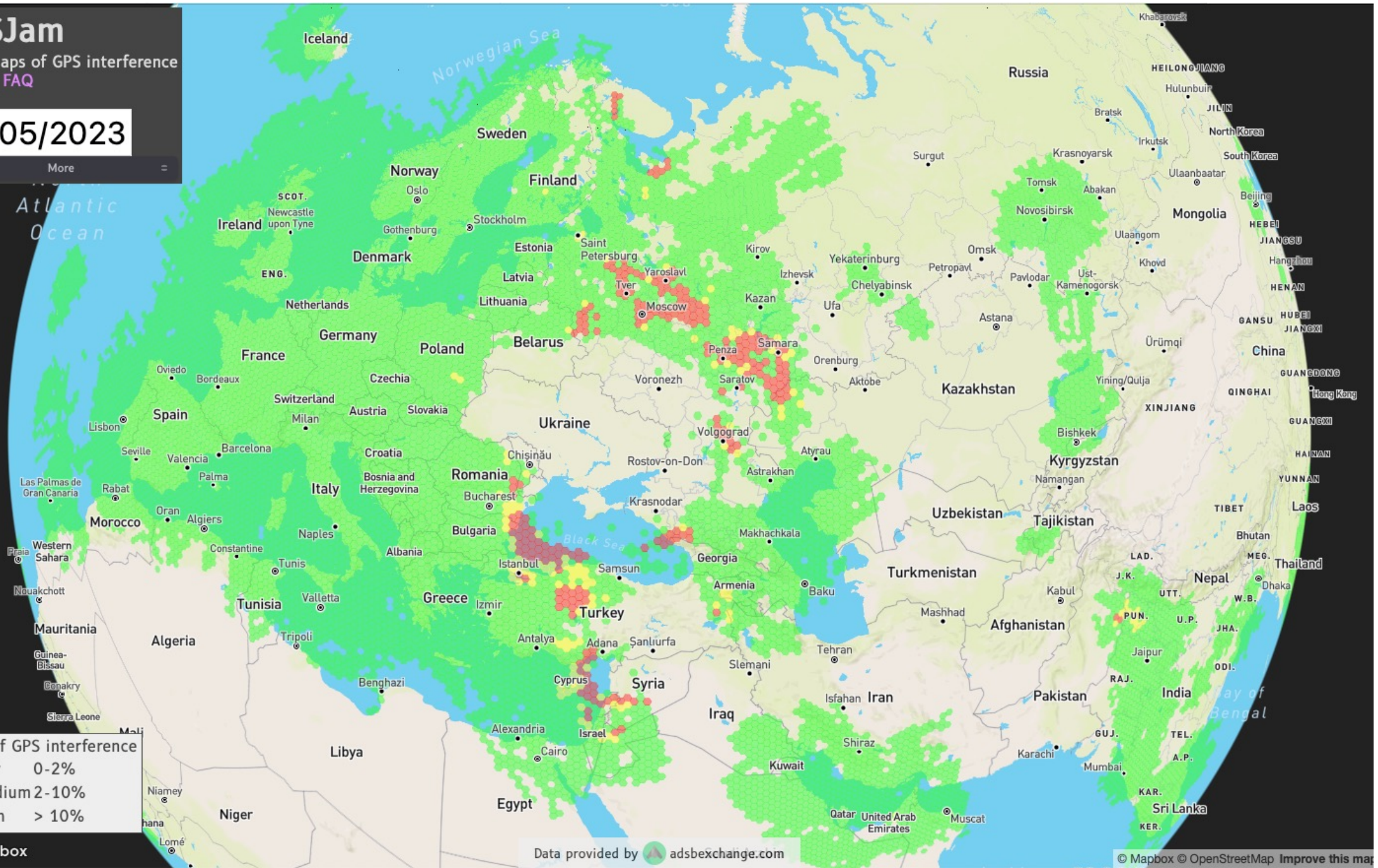
Level of GPS interference

- Low 0-2%
- Medium 2-10%
- High > 10%

mapbox

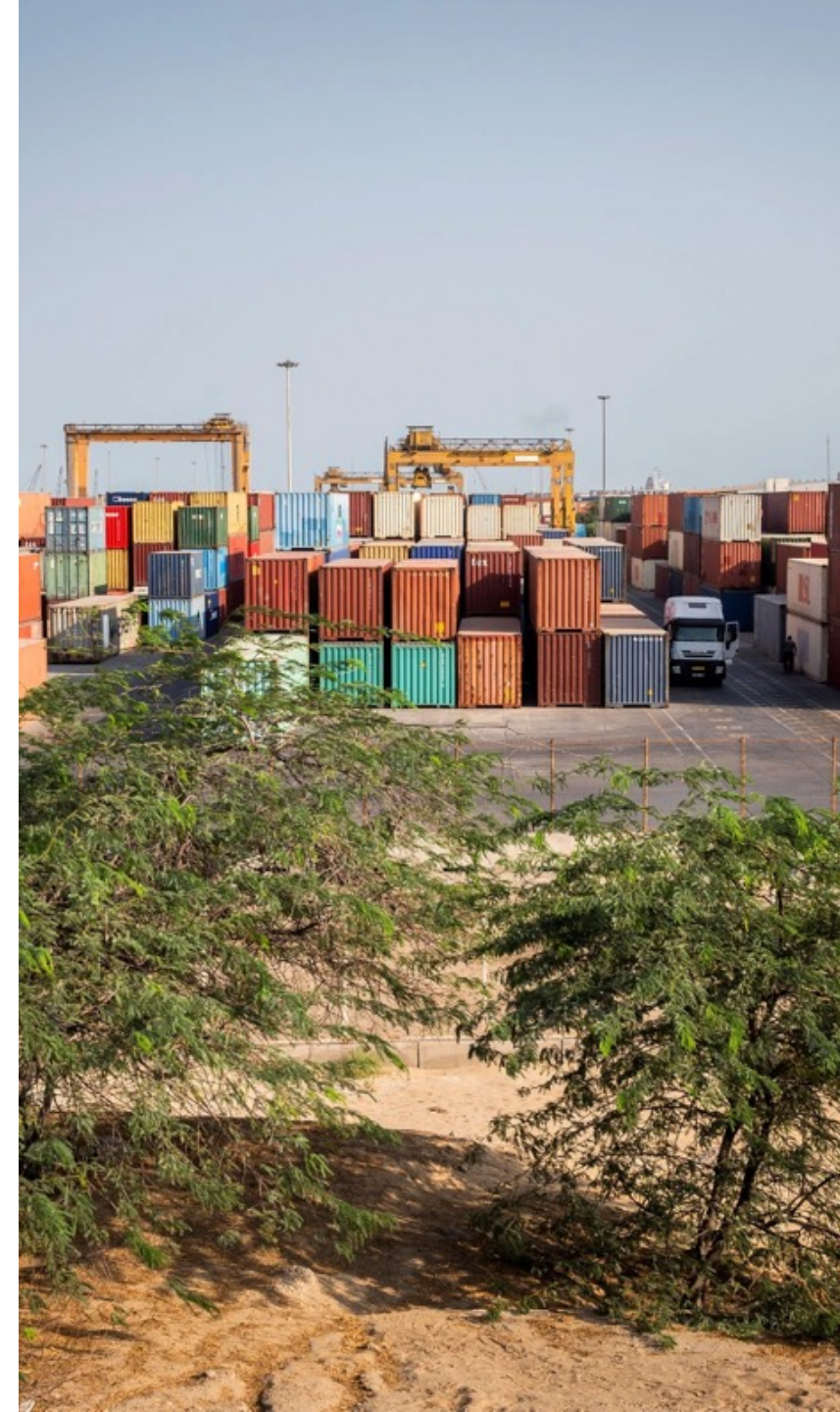
Data provided by [adsbexchange.com](#)

© Mapbox © OpenStreetMap Improve this map



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



BRANDON BELL/GETTY IMAGES

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...'



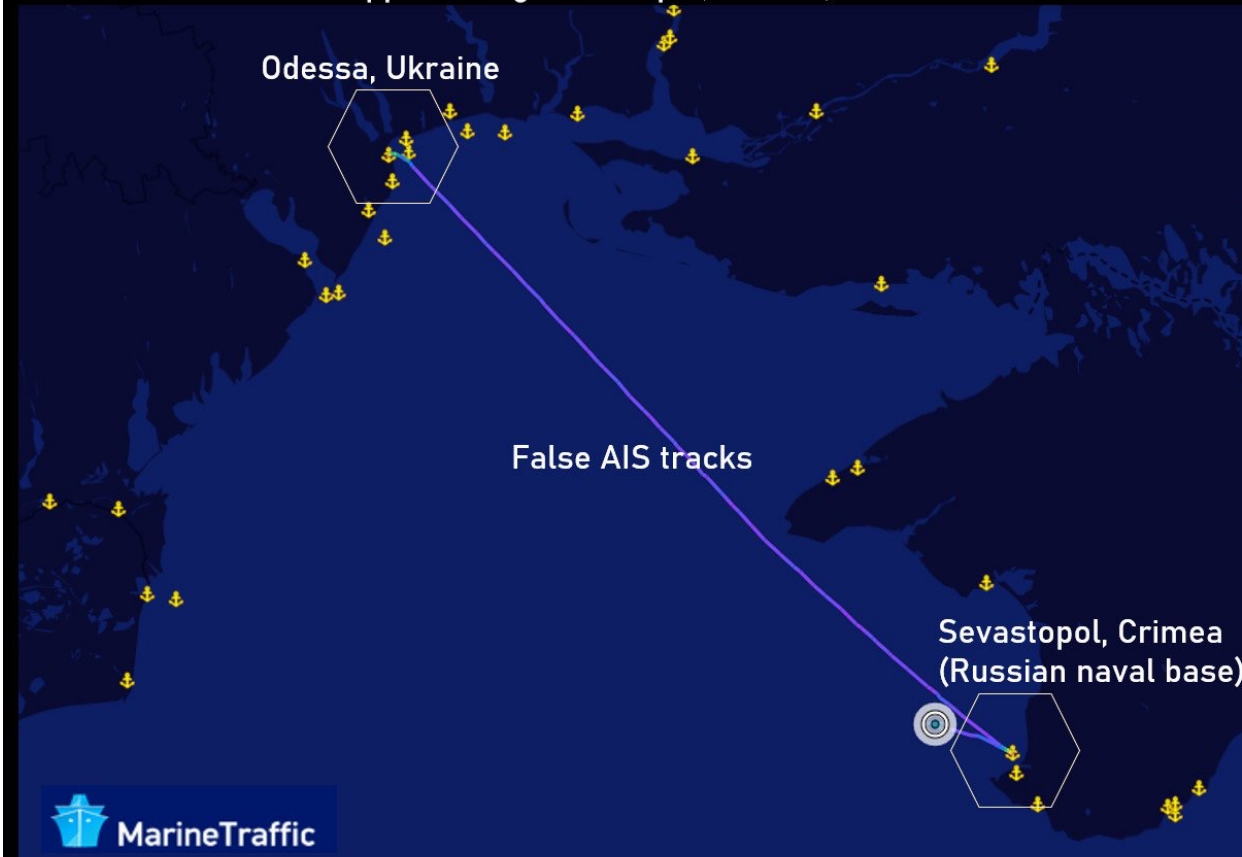
Saving money using cryptocurrency swaps

Ziggo
zakelijk

2 maanden
Gratis

AIS spoofing (usni.org 2021)

Falsified AIS (Automated Identification System) appearing to show HMS Defender and HNLMS Evertsen approaching Sevastopol, Crimea, On June 19 2021



Webcams showing HMS Defender (A) and HNLMS Evertsen (B) in Odessa



Russian Invasion of Ukraine

- KillNet is a Russia-aligned hacktivist group.
- Similar to the Ukrainian Digital Army they use telegram channels to coordinate cyber attacks.
- They have targeted European ATC, European Parliament and US government targets.
- They targeted also ships used to bring US equipment to Ukraine and NATO deployments in Eastern Europe.



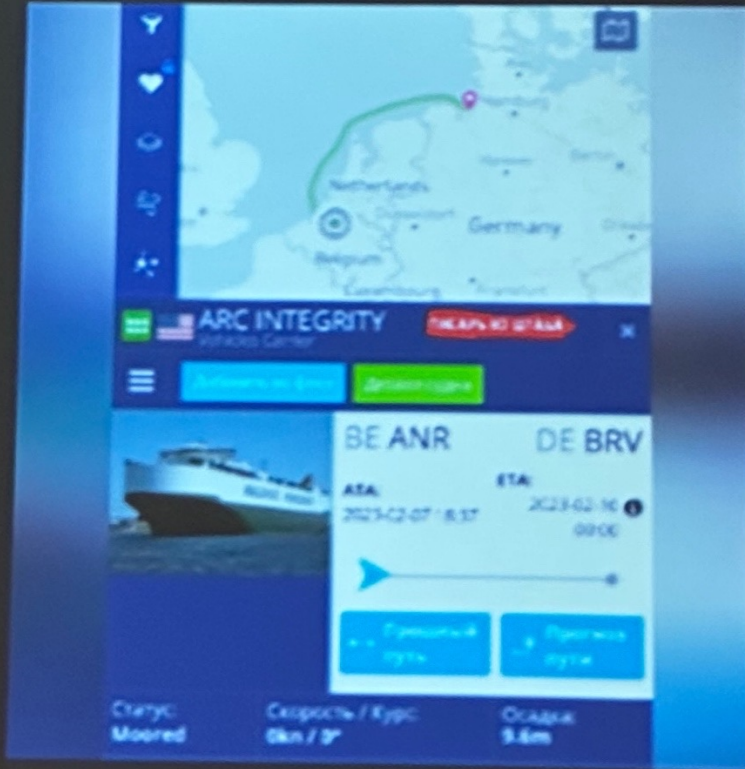


KILLNET CHAT

10 050 members, 802 online



Forwarded from Clerk from the Headquarters



» The M2 Bradley armored personnel carrier in the transport and cargo vessel ARC Integrity (USA) is now in the Belgian port of Antwerp. the intermediate point is the port of Bremerhaven, Germany. It is on this ship that Bradley goes to the crests. What prevents our DRG from sinking a bulk carrier? (avenge the Novorossiysk in 1955m) Technically

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.

Security

Maritime giant DNV says 1,000 ships affected by ransomware attack

Carly Page @carlypage_ / 3:39 PM GMT+1 • January 18, 2023

 Comment

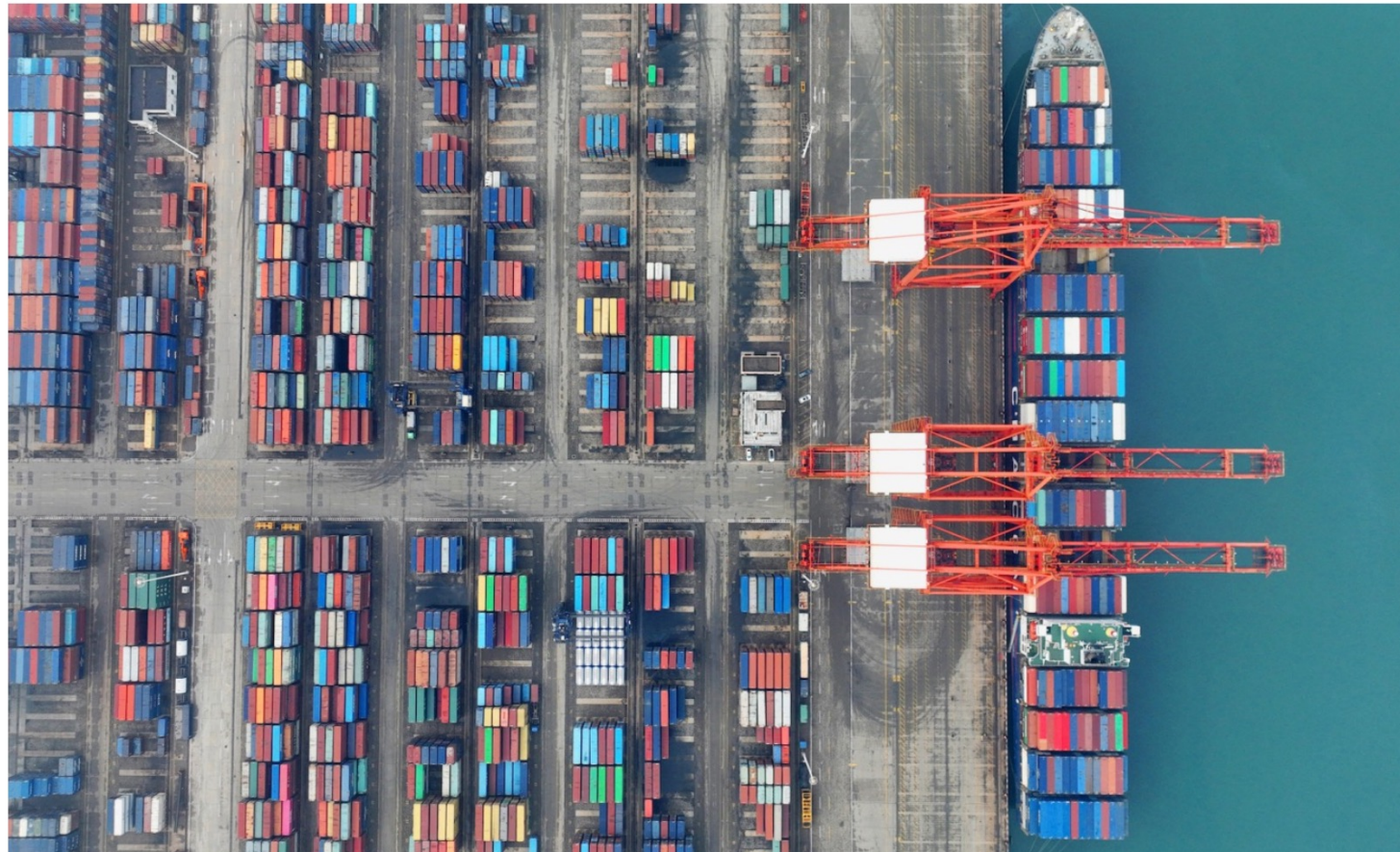


 Image Credits: STR / AFP / Getty Images

Home » Nieuws » Russische cyberaanvallen op Nederlandse havens – FERM monitort

Russische cyberaanvallen op Nederlandse havens – FERM monitort

📅 14 juni 2023

📌 Cyberweerbaarheid FERM

🕒 6min.

FERM heeft op dinsdag 6 juni jl. dreigingsinformatie ontvangen waaruit duidelijk werd dat er op dat moment lopende DDoS-aanvallen uitgevoerd werden op havens. De aanvallen werden (en worden) actief in de gaten gehouden, waarbij onze participanten via het portal door elkaar en door FERM op de hoogte worden gehouden. Inmiddels zijn deze aanvallen per vandaag ook in de landelijke media belicht, waardoor we er nu op onze openbare website ook aandacht aan besteden.

Deel dit bericht



Russian hackers block websites in retaliation for Leopard tanks

June 14, 2023




Rotterdam harbour. Photo: Quistnix via Wikimedia Commons

Pro-Russian hackers have been blamed for forcing the websites of Dutch commercial ports offline last week.

Groningen Zeehaven's site was down all weekend, while Amsterdam, Rotterdam and Den Helder were all offline for several hours on Tuesday.

1:44 M LS P • 📶 🔋

←  **NoName057(16) Eng**
1.5K subscribers

🎉 2 👍 1

👁️ 272 6:58 AM

💬 Leave a comment >

We sent to rest the website of the Port Authority of Quebec:

✖️ <https://check-host.net/check-report/f874c8ek4b1>

👉 Subscribe to NoName057(16)
👤 Join our DDoS-project
⚠️ Subscribe to reserve channel

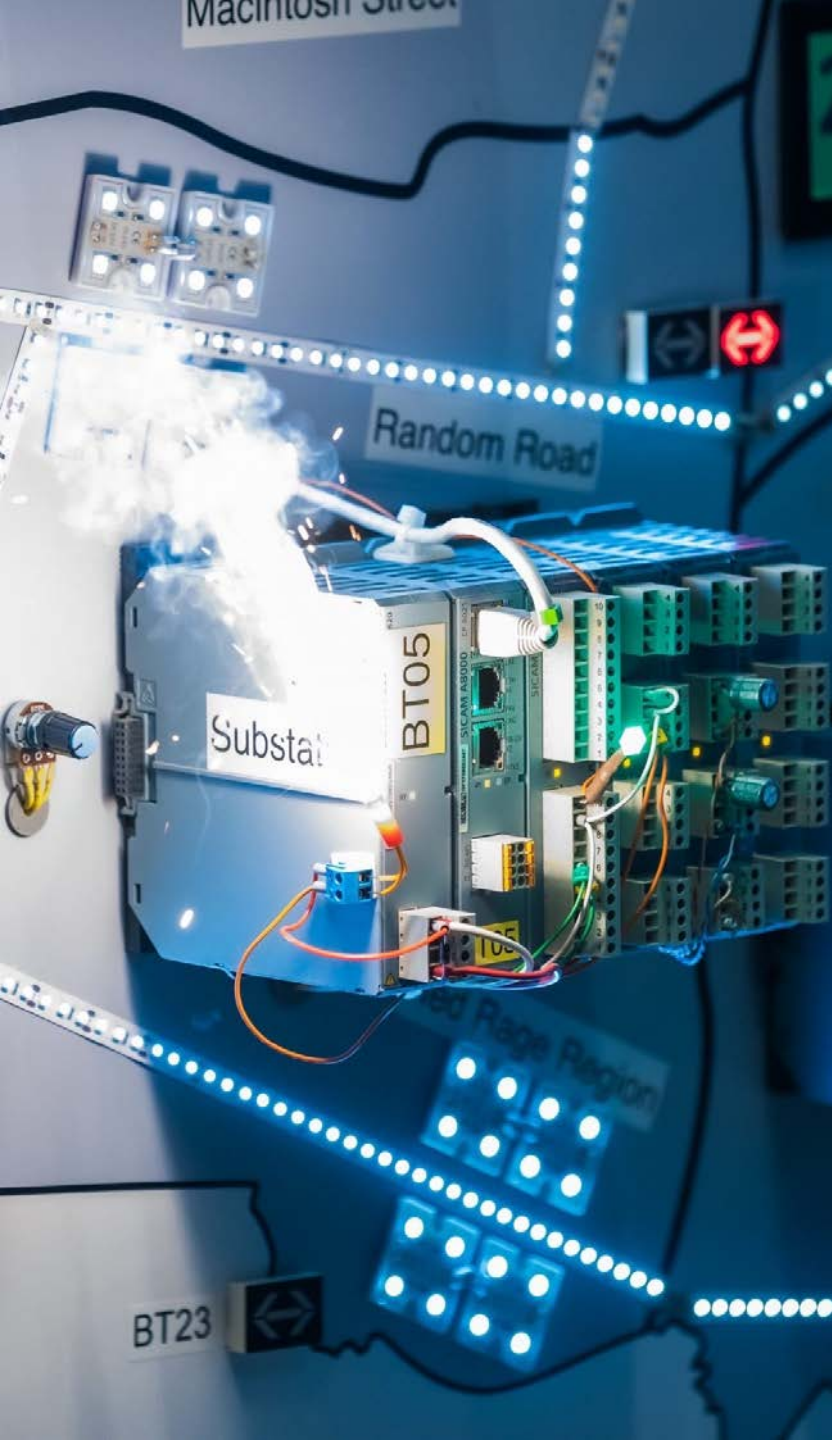
🇷🇺 Victory will be ours!

👍 1 🎉 1

👁️ 255 7:46 AM

💬 Leave a comment >

MUTE

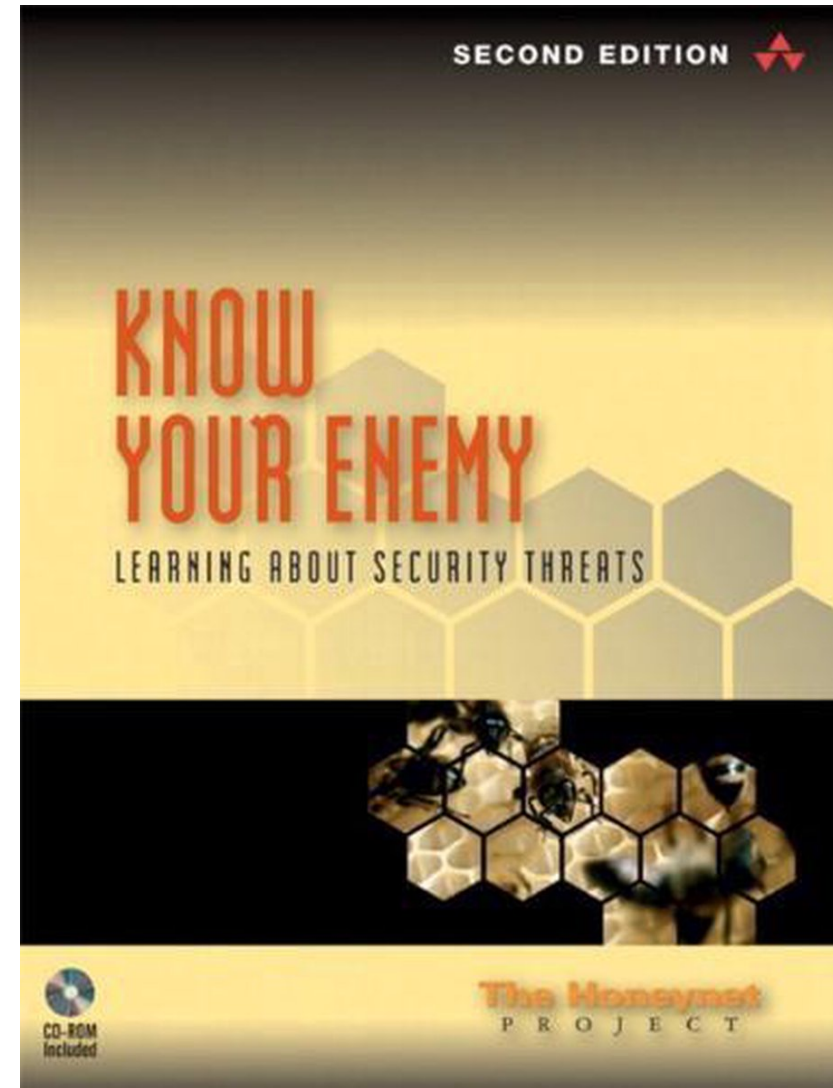


Create Maritime Technology Hacking Lab

- 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



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



Track

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

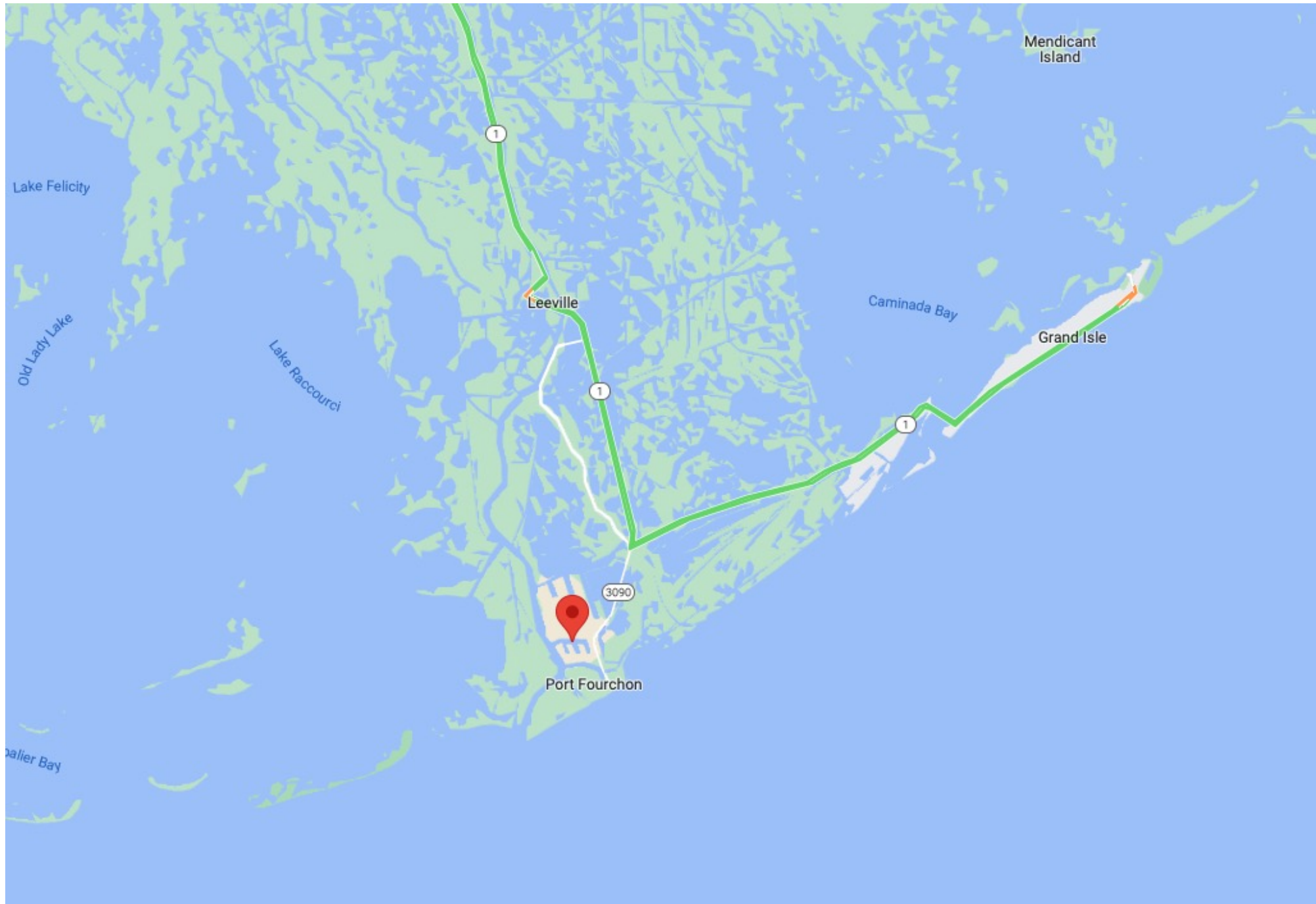
Modem: GMXP:
 Net Power
 Tx Status
 Rx1 ADU power
 Rx2 CM power
 Status

Ship

Latitude: 29.121323 N degree
Longitude: 90.203781 W degree

Antenna

Cross Level: -0.0 degree



Mendicant Island

Lake Felicity

Old Lady Lake

Lake Raccourci

Leeville

Caminada Bay

Grand Isle

Port Fourchon

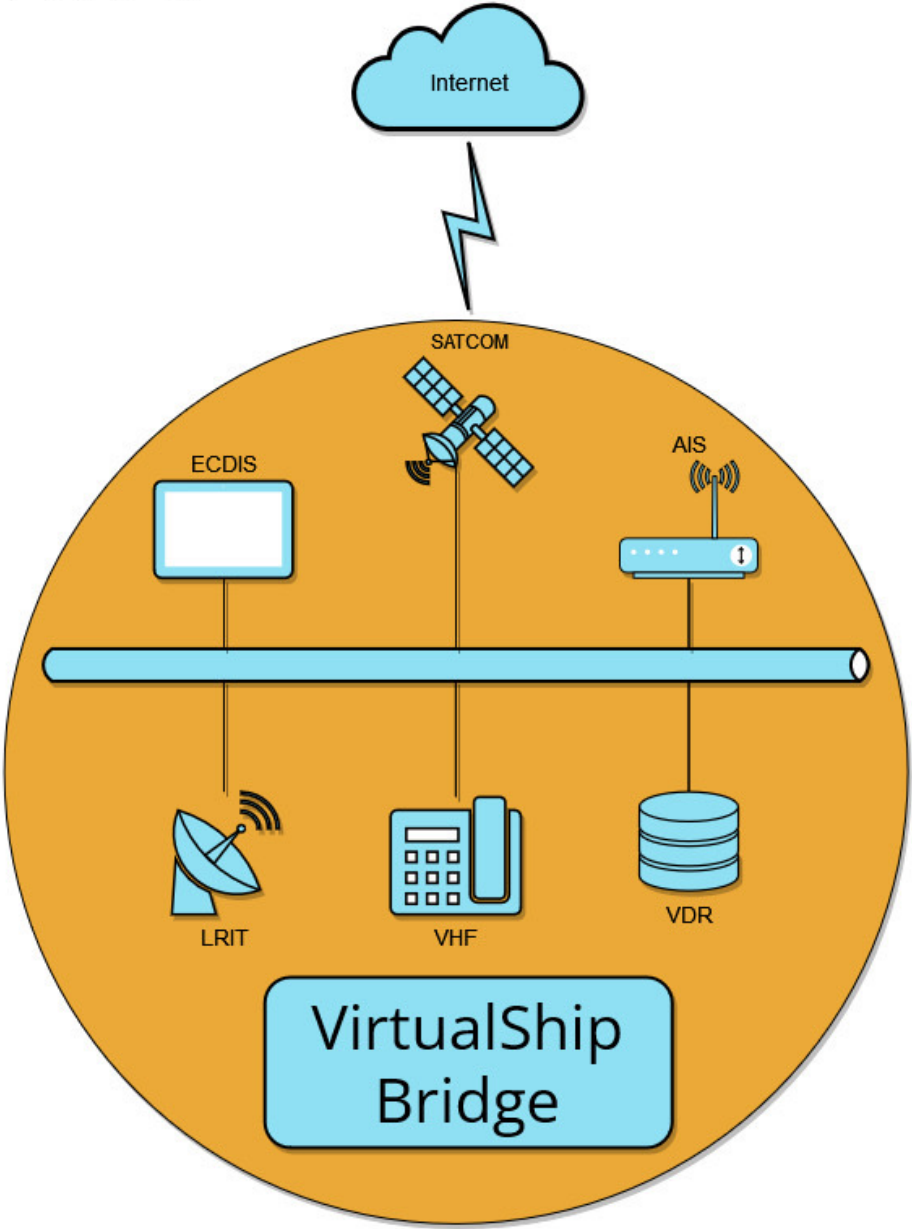
Palier Bay

1

1

1

3090



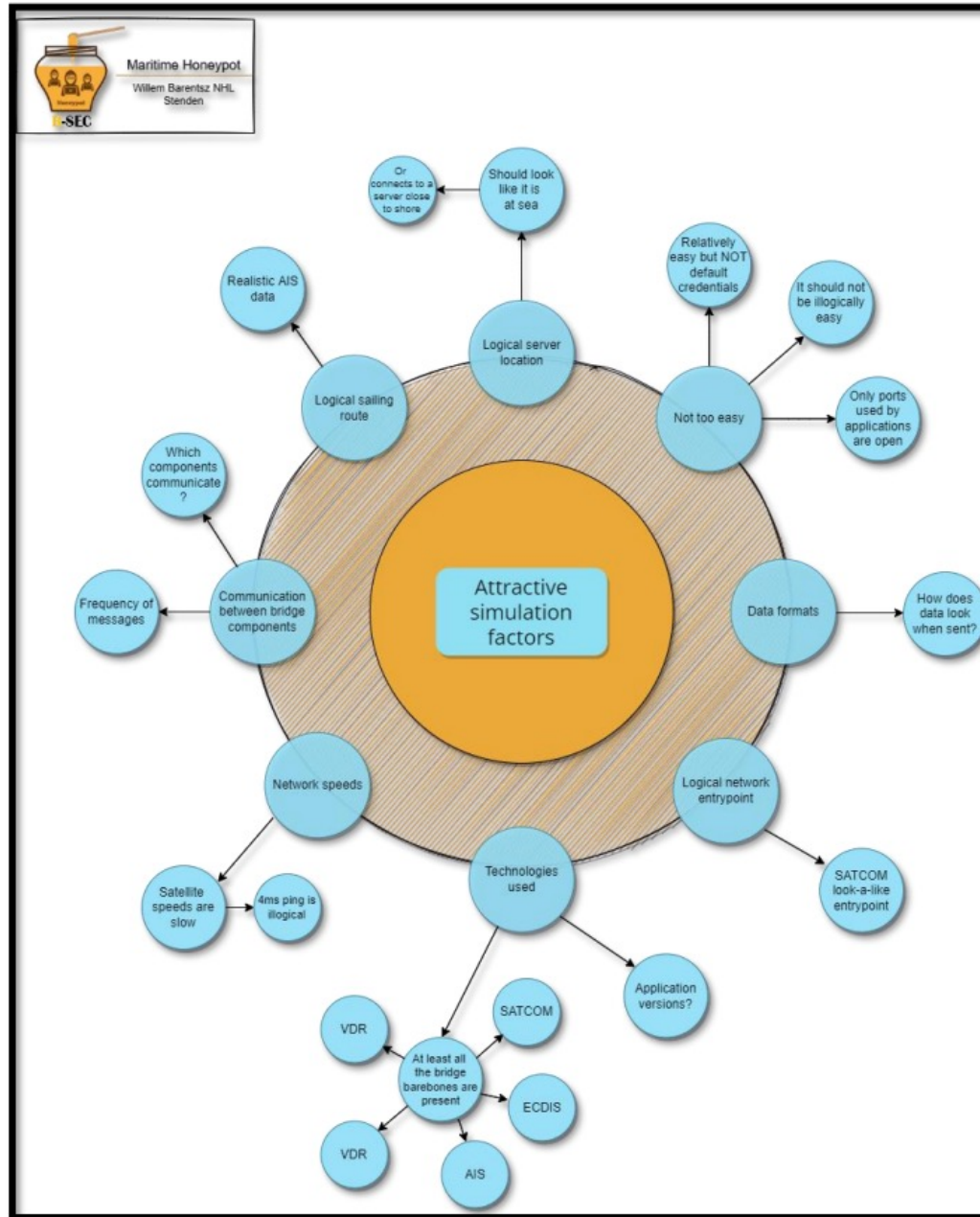


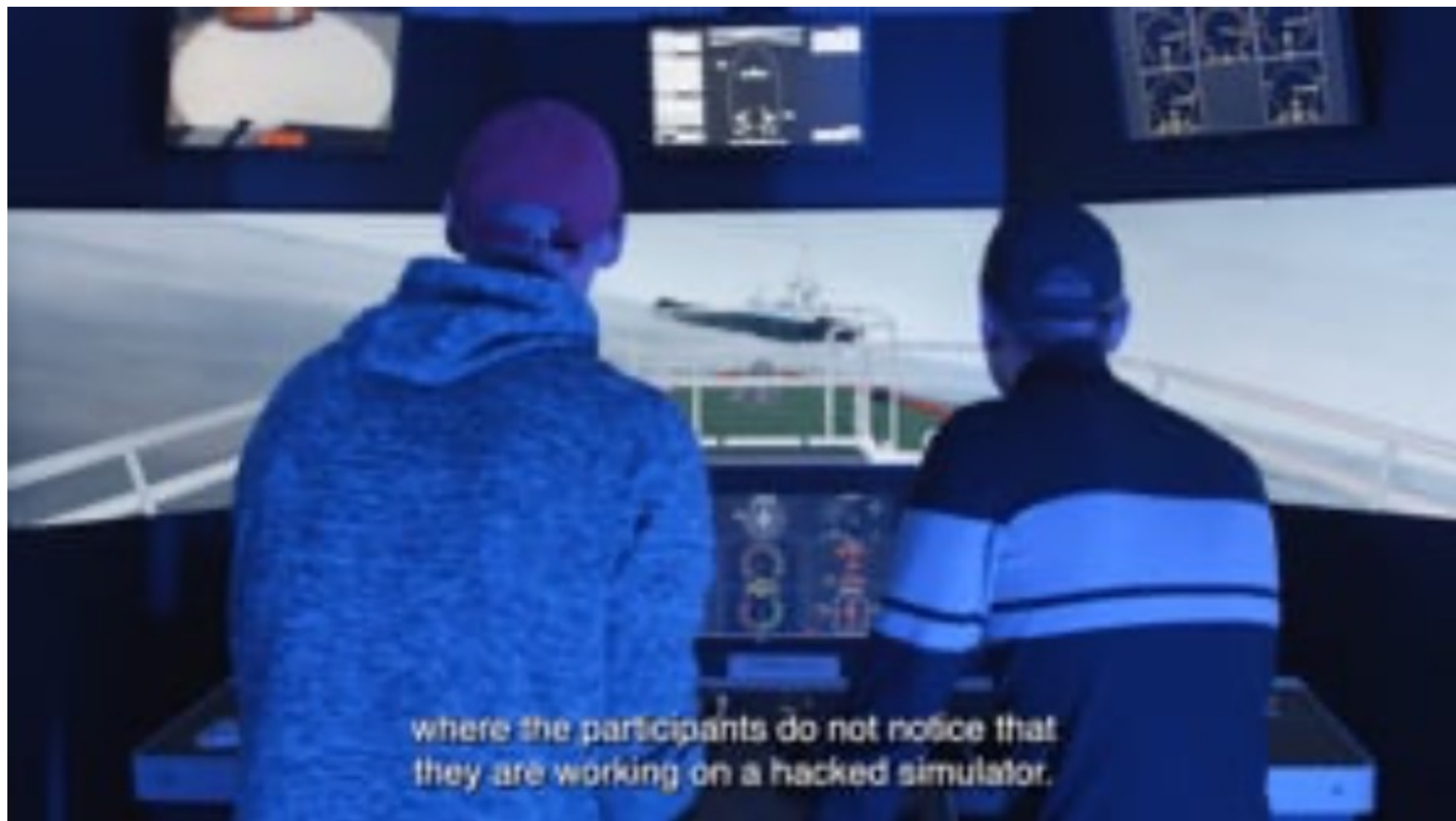
Figure 4 – Mindmap attractive simulation factors.



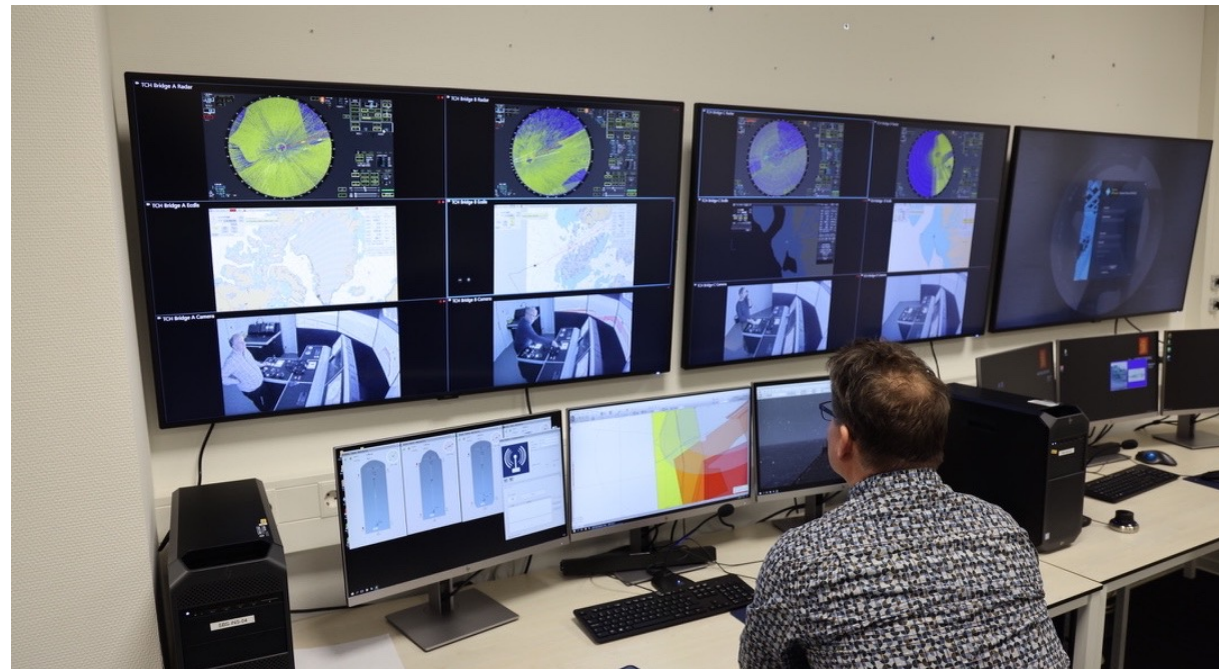
Maritime Cyber Incident Simulations

- 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





where the participants do not notice that they are working on a hacked simulator.



Threat	Deviation of electronic position due to cyberattack on ECDIS/GPS
Materials used	<ul style="list-style-type: none"> ● Introduction exercise ● Simulator ● Ship model CNTRN43.B ● Deviation of electronic position ● Flowchart/Game Martin ● Research/observation form ● Evaluation form
Scenario research questions	<p>Observations: (What do we want to investigate and why?)</p> <p>The effect of actions in whether or not to register deviation to navigation equipment such as the ECDIS.</p> <p>Research questions:</p> <ul style="list-style-type: none"> - 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?





Show Caption ▾

SAN FRANCISCO — Was a hack attack behind two separate instances of Navy ships colliding with commercial vessels in the past two months? Experts say it's highly unlikely, but not impossible — and the Navy is investigating.

Rumors on Twitter and in computer security circles have been swirling about the possibility that cyber attacks or jamming were involved in the collisions. Speculation has been fueled by four accidents involving a U.S. warship this year, two of which were fatal, the highly-computerized nature of modern maritime navigation, and heightened concern over global cyberattacks — especially attacks against U.S. government entities.



The damaged port aft hull of USS John S. McCain, is seen while docked at Singapore's Changi naval base on Aug. 22, 2017 in ... [Show more](#) ▾
WONG MAYE-E, AP

USNavyCNO @USNavyCNO · [Follow](#)

2 clarify Re: possibility of cyber intrusion or sabotage, no indications right now...but review will consider all possibilities

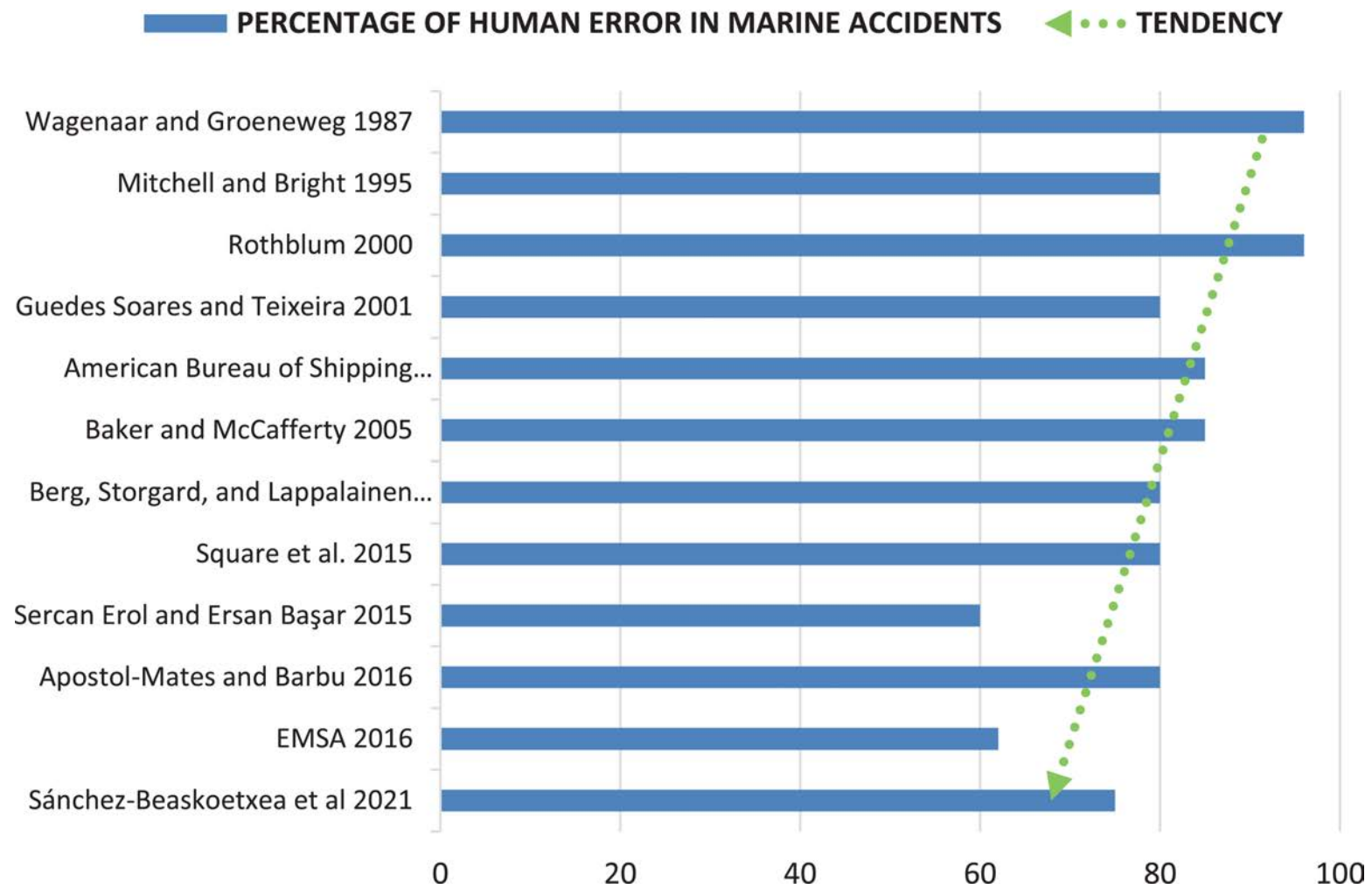
10:04 PM · Aug 21, 2017

1.2K Reply Share

[Read 118 replies](#)

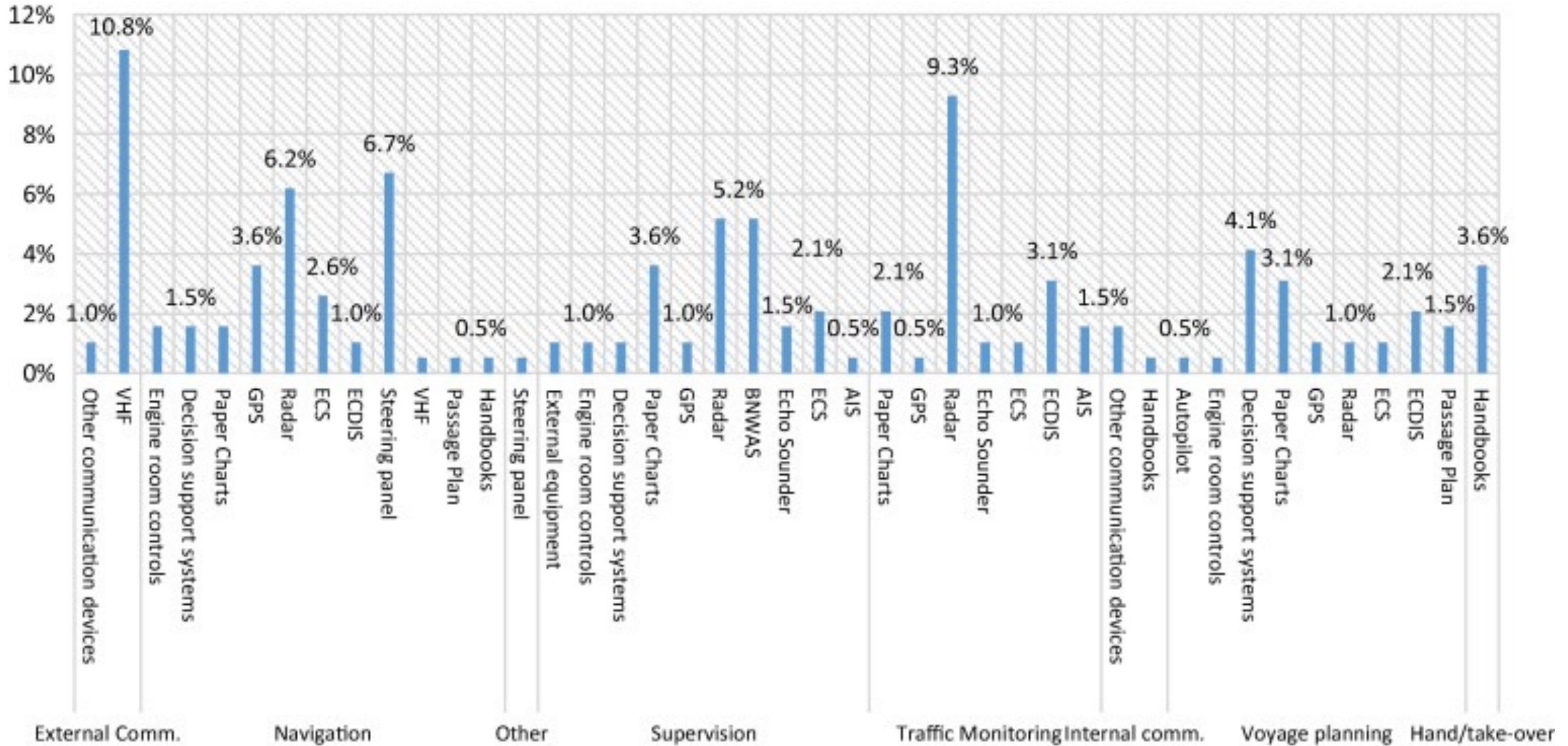


Percentage of human error in marine accidents according to several authors.



Javier Sánchez-Beaskoetxea et al 2021

Percentage of technical equipment involved, divided by task error category.



Netherlands Coast Guard Dilemma Session Agenda

1300 – 1345

- Introduction

1345 – 1400

- Incident Conduct & Scenario Intro

1400 – 1430

- Part 1 0600 HRS

1430 – 1500

- Part 2 1200 HRS

1500 – 1530

- Part 3 1800 HRS

1530 – 1545

- Press conference role play

1545 – 1630

- Exercise Wash-up/Wrap up

Scenario Introduction

- Ruthenia is an Eastern European major power whose President, Igor Talin, wants to return Ruthenia to its superpower status of the past.
- One of Ruthenia's neighbours is Orangeland.
- Orangeland has a new West leaning government with ambitions for closer ties with the EU and NATO.
- Igor Talin is opposed to this, and tensions led to a Ruthenian military invasion of Orangeland.



Ruthenian and the Netherlands

- The Netherlands have provided political support and military aid to Orangeland.
- The Netherlands government have accused Ruthenia of war crimes.
- In recent weeks the Netherlands have sent tanks to Orangeland purchased from allies.
- Ruthenian military bloggers have said the Netherlands will regret this interference.



Ruthenia

- Ruthenian has a significant Navy and uses it to project its power
- Ruthenian SSS (State Security Service) hackers are highly skilled and responsible for many attacks against Western countries.
- It has also conducted serious disruptive attacks on the power grid of Orangeland in the years leading up to the recent invasion.



ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

February 6, 2023

CYBER

The Orangeland war was the key factor in Ruthenia's cyber operations prioritization in 2022. Although its cyber activity surrounding the war fell short of the pace and impact we had expected, Ruthenia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Ruthenia views cyber disruptions as a foreign policy lever to shape other countries' decisions.

- Ruthenia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.



April 1, 2023
Washington, D.C.

Safety Alert 04-23

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

In March 2023, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities.

Prior to the incident, the security risk presented by the shipboard network was well known among the crew. Although most crewmembers didn't use onboard computers to check personal email, make online purchases or check their bank accounts, the same shipboard network was used for official business – to update electronic charts, manage cargo data and communicate with shore-side facilities, pilots, agents, and the Coast Guard.

It is unknown whether this vessel is representative of the current state of cybersecurity aboard deep draft vessels. However, with engines that are controlled by mouse clicks, and growing reliance on electronic charting and navigation systems, protecting these systems with proper cybersecurity measures is as essential as controlling physical access to the ship or performing routine maintenance on traditional machinery. It is imperative that the maritime community adapt to changing technologies and the changing threat landscape by recognizing the need for and implementing basic cyber hygiene measures.

In order to improve the resilience of vessels and facilities, and to protect the safety of the waterways in which they operate, the U.S. Coast Guard **strongly recommends** that vessel and facility owners, operators and other responsible parties take the following basic measures to improve their cybersecurity:

- **Segment Networks.** “Flat” networks allow an adversary to easily maneuver to any system connected to that network. Segment your networks into “subnetworks” to make it harder for an adversary to gain access to essential systems and equipment.
- **Per-user Profiles & Passwords.** Eliminate the use of generic log-in credentials for multiple personnel. Create network profiles for each employee. Require employees to enter a password and/or insert an ID card to log on to onboard equipment. Limit access/privileges to only those levels necessary to allow each user to do his or her job. Administrator accounts should be used sparingly and only when necessary.



Europe



2 minute read · February 20, 2023 12:49 PM GMT+1 · Last Updated 16 days ago



Ruthenia targets Netherlands' North Sea infrastructure, says Dutch intelligence agency

Reuters



Wind turbines are seen at the North Sea in Scheveningen, Netherlands August 25, 2022.

REUTERS/Piroschka van de Wouw

THE HAGUE, Feb 20 (Reuters) - Ruthenia has in recent months tried to gain intelligence to sabotage critical infrastructure in the Dutch part of the North Sea, Dutch military intelligence agency MIVD said on Monday.

A Ruthenian ship has been detected at an offshore wind farm in the North Sea as it tried to map out energy infrastructure, MIVD head General Jan Swillens said at a news conference.

The vessel was escorted out of the North Sea by Dutch marine and coast guard ships before any sabotage effort could become successful, he added.

NEW TAILOR

Maak jouw garderobe nu klaar voor alle momenten van de week

MAAK EEN AFSPRAAK

MEER INFORMATIE

Report an ad



Register for free to Reuters and know the full story

Register now

S&P Global
Commodity Insights

**In a changing market,
find your constant.**





Hoek van Holland, IJmuiden, Texel, Rottum

The weatherforecast for Netherlands Hoek van Holland, IJmuiden, Texel, Rottum.

Issued: 27 april 2023 00:26

Forecast valid from 01:00 to 13:00

Flushing Hoek van Holland, IJmuiden, Texel, Rottum

north to northwest 3-4, soon becoming northwest 4-5, later increasing 7-8.

First change of light rain or drizzle. visibility moderate, sometimes poor, first chance of fog, increasing to good.

Forecast valid from 13:00 to 01:00

Flushing Hoek van Holland, IJmuiden, Texel, Rottum

northwest 4-5, becoming northwest 7-8, later decreasing 5-6. later rain. visibility good, in precipitation moderate.

A further report will be issued by 06:00 on Thursday, 27 April 2023.

All times are in local time.

Delen via




Meer informatie

[Marifoonbericht](#) →

[Scheepsweerbericht](#) →

[Dutch Continental Shelf](#) →



No.1	Name vessel:	OOCL Rauma
	Callsign:	PBWS
	Length/width:	169 m / 27 m
	Draft:	9,30 metre
	Persons on board:	15
	Destination:	Helsinki Via NOK
	Position:	52° 10, 32 North 003°54,4 East 1,5' east Oil rigg P15E
	Course	351°
	Speed	drifting
	Cargo	General cargo in containers
	Dangerous cargo:	Yes
	Picture:	
	Owner:	JR Shipping (Dutch)
	Flag	Dutch
	IMO	9462794
	MMSI	246650000



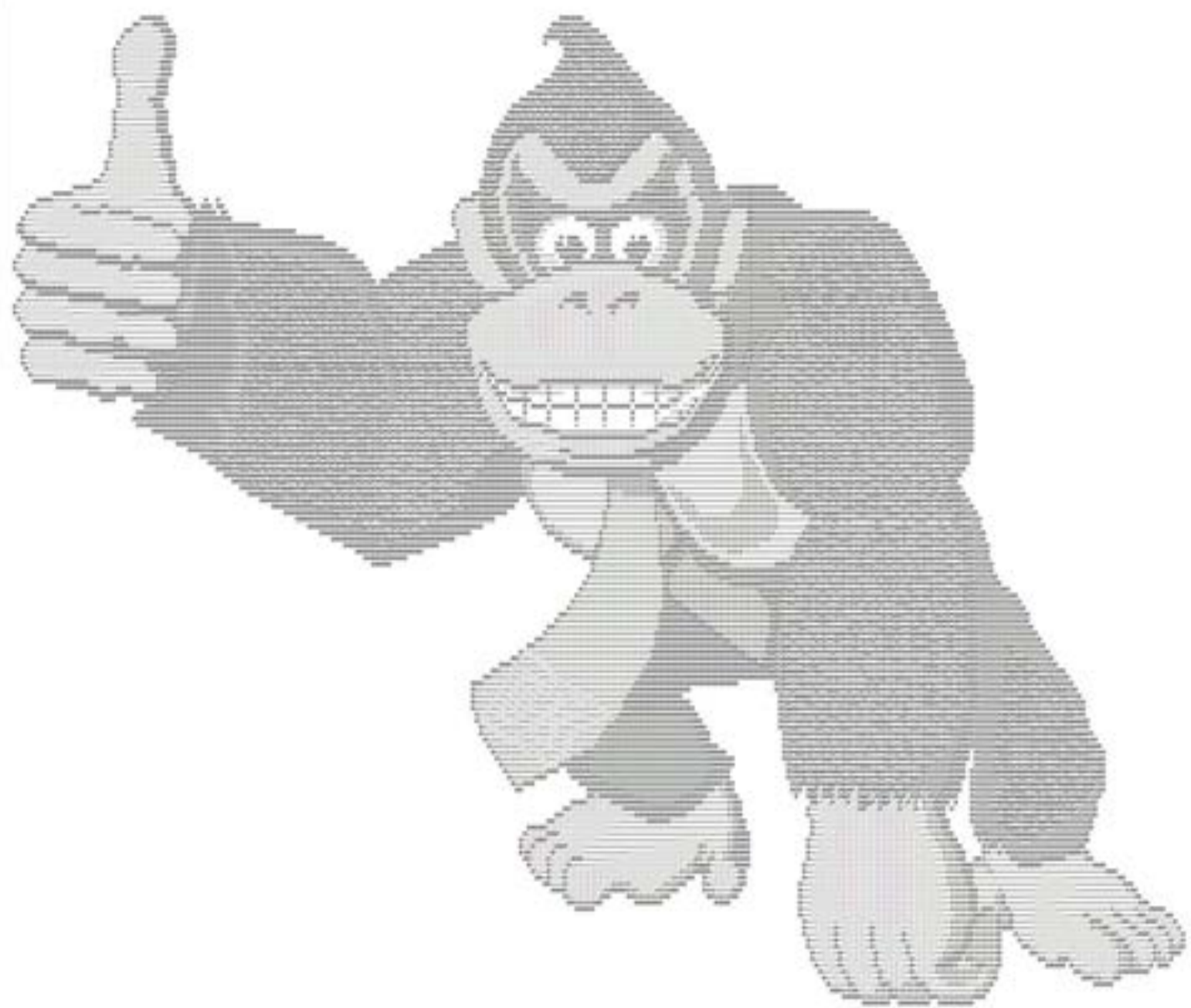
Repairing file system on C:

The type of the file system is NTFS.

One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.

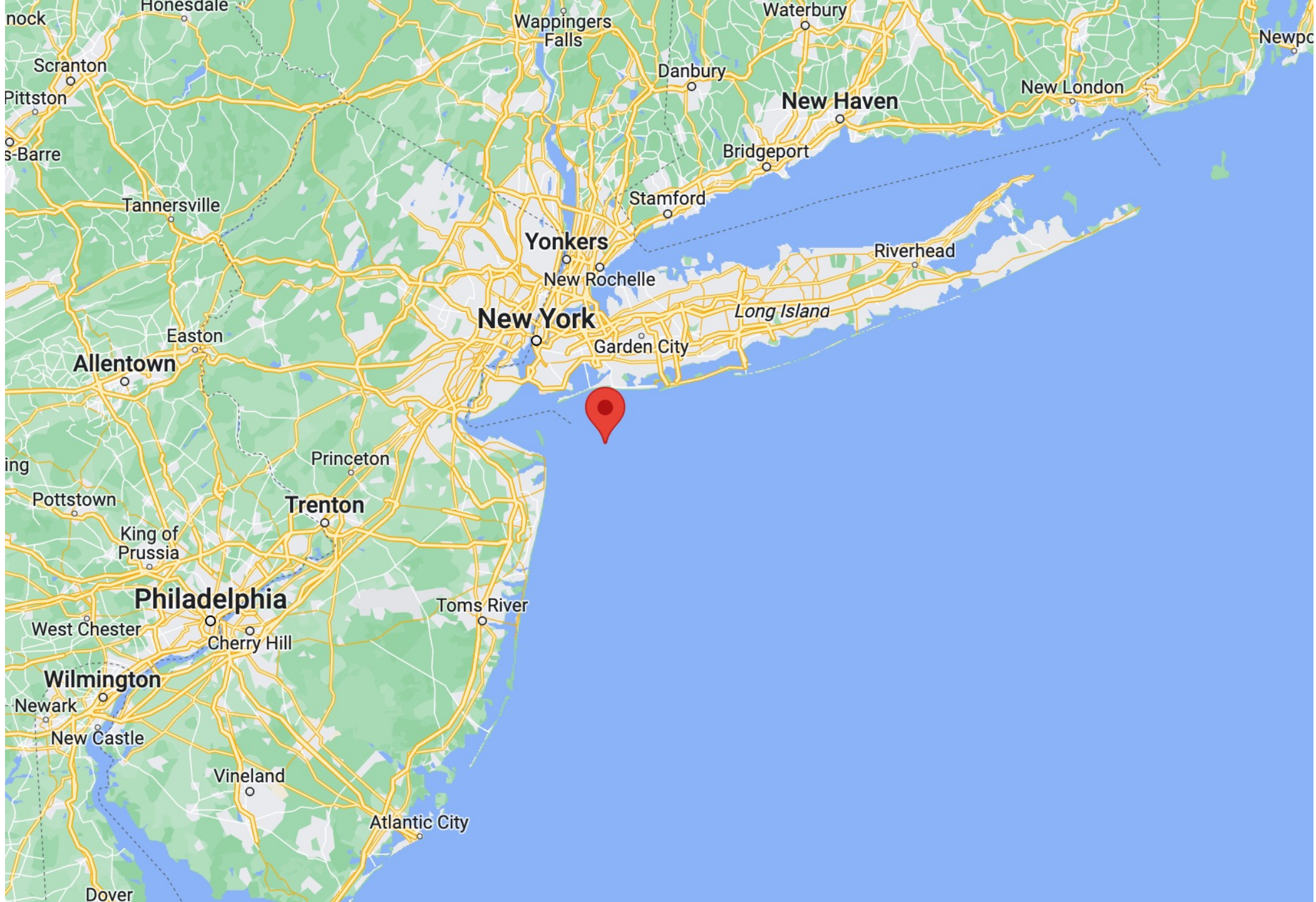
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!


CHKDSK is repairing sector 22848 of 380384 (6%)









No.3	Name vessel:	Eternal Resource
	Callsign:	VRQS6
	Length/width:	254 m/ 43 m
	Draft:	11,5 m
	Persons on board:	25
	Destination:	New York
	Position:	40° 26, 32 North 073°45,45 West
	Course	var
	Speed	stopped
	Cargo	Bulk Coal 95.000 ton
	Dangerous cargo:	No
	Picture:	 <p>The image shows the bulk carrier ship 'Eternal Resource' from a starboard perspective. The ship has a dark red hull and a white superstructure. The name 'ETERNAL RESOURCE' is visible on the side of the hull. The ship is on the water, and the sky is clear and blue. A small watermark in the bottom left corner of the image reads '© Iwan Afwan MarineTraffic.com'.</p>
	Owner:	DAIICHI CHUO MARINE - TOKYO, JAPAN
	Flag	Hong Kong
	IMO number	9515187
	MMSI	477045300







KINGKONG TECHNICAL ANALYSIS

LogRhythm Labs

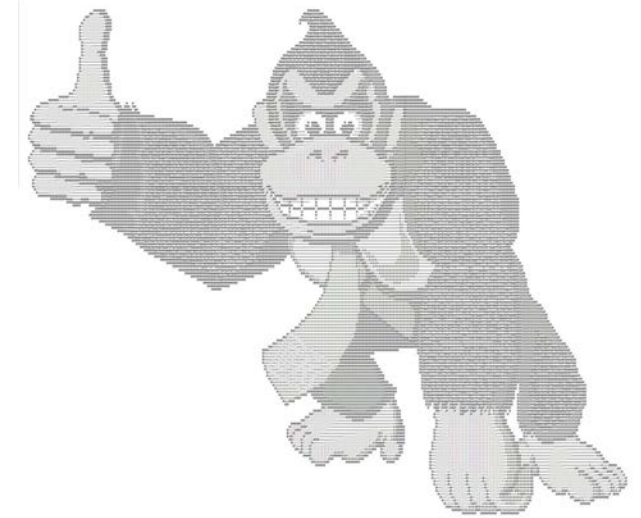
April 2023



LogRhythm[®]

The Security Intelligence Company

KingKong Malware Analysis



- Initially, analysis showed many similarities with other ransomware samples from 2022, but further research indicated the malware had been modified to cause data destruction.
- KingKong overwrites or encrypts sectors of the physical hard drive and C: volume, but it does not contain the ability to restore the files, rendering recovery impossible even if the ransom is paid.
- KingKong also has the ability to send messages to Autopilot before wiping drives.



The Ruthenian Cyber Army @TheRuthenianCyberArmy .1h

Dutch vessels under attack by the Ruthenian Cyber Army



Telegraaf.nl

Dutch vessels under attack by the Ruthenian Cyber Army

A report from the Dutch cybersecurity service reveals insight into what the country has been facing from belligerent attackers and holds a ...

66

107

246

43.9K



TOP STORIES



Russian Subsea Construction Vessels Draw Scrutiny Off Ireland



Yara and Enbridge to Develop Large Blue Ammonia Project at Texas Port



Carrier USS Ford Passes Key Test in Preparation for First Deployment



South Korea's FTC Becomes Holdout to Approval of Hanwha-DSME Deal

Dutch vessels under attack by Ruthenian Cyber Army

TRENDING STORIES

China is Preparing Merchant Ro-Ro Ferries for Amphibious Warfare

US Navy Donates its Last Two Cyclone-Class Patrol Ships to Philippines

U.S. May Not Have Enough Mariners Available to Mobilize Sealift Fleet

Greek Ship Manager Pleads Guilty to MARPOL Charges

EDITORIALS

Study: Torrents of Antarctic Meltwater are Slowing Ocean Currents

Facing \$2M Fine, Port of Morrow Contends With Another Wastewater Spill

For Indo-Pac Islands, Sea Level Matters More Than US-China Rivalry

Join the conversation.



FEATURED STORIES

ABS Wavesight, Meteomatics Present the Power of Elevated Weather Data

Digitalize Your Bunkering Transactions With Moorio

The Blue MBA is Fulfilling Aims to Stay Relevant, Current and 'Green'

BLOGS +

PODCASTS +

MORE TOP STORIES



Allision Damage Forces Indonesian Ferry to Intentionally Run Aground



Lauritzen and Cargill Expand Methanol-Fueled Bulker Orders from Japan

Rotterdam Harbour appears to be the source of cyber attack spread



Cybersecurity service report reveals insight into what has been attacking Dutch vessels and source of the att..

26 Apr 2023

J. Lauritzen Orders Two Methanol Dual-fuel Bulk Carriers



24 Apr 2023

Norled's Hydrogen-powered Ferry Enters Service

25 Apr 2023

Gulf of Guinea Tanker Hijacking: Pirates Abandon Ship, Take Some Crew Members with Them



23 Apr 2023

WSF Invites Bids to Convert Its Largest Ferries to Hybrid-electric

Latest Maritime News

Venezuela's March Oil Exports Rise on More Supertankers, Chevron Cargoes

Venezuela's oil exports rose in March to the highest monthly average...

Industry Welcomes EU's Decision on Filipino Seafarer Certificates

The European Commission has decided to continue recognising certificates...

Three Austal USA Executives Indicted for Fraud

A federal grand jury returned an indictment last week charging three...

Next IMO Secretary-General Could be a Win for Diversity

Seven IMO Member States have nominated a candidate for the post of...

FMD's New High-speed Engine to be Tested for US Navy's LUSV Platform

Fairbanks Morse Defense (FMD) announced it has been contracted to...

Gladding-Hearn Delivers Refitted Launch to

NL Police Forensic Report



- The Netherlands Police have identified the source for the KingKong wiper-malware infection on Kings Day 2023. This was based on intelligence received from the FBI liaison officer in the Hague.
- This intelligence led a search warrant being executed at the Rotterdam offices of Limany Group.
- Limany Group supply ship chandlery services to a number of shipping lines.
- It appears they handled all the impacted ships when they were in the port of Rotterdam.



Acting director - Dutch Coast Guard Edwin van der Pol



Current Cyber Threats to Maritime Security

Webinar – 13th April 2022

NHL
STENDEN
university of
applied sciences



NHL
STENDEN
hogeschool



any talk about our influence



- Build the environment using equipment from maritime industry:
 - Raspberry Pi
 - Software Defined
- Based on known issues from other CS/CSSCA-issues and conduct vulnerability research in lab environment
- Build a virtual ship Hologram to study current active warning
- Use discovered vulnerabilities and Hologram data to develop:
 - Research report/publication
 - Report vulnerabilities
 - Issues to marine cyber incident simulator



OTV
News Flash

Port of Orangeland Cyber-attack

Questions



university of
applied sciences