

Threats to Maritime Security: Cyber & Nexus to Piracy

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 \uparrow CO₂ 154,712 t

FREIGHT \square Containers 14,737,118 \triangle Dry 579,195 kt flame Liquids 420,788 kt gas Gas 63,241,080 m³ car Vehicles 10,507,073 kt

OPTIONS Show \downarrow Colours \downarrow Filters \downarrow



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).



Maritime Cyber Surveys

- BIMCO/Safety at Sea Survey 2020 said 31% of maritime organisations experienced a cyber incident up from 24% in 2019
- 52% said people were their biggest cyber vulnerability compared to 17% their IT systems
- Only 16% conduct cyber attack drills for staff
- In a 2022 survey sponsored by International Chamber of Shipping reported a higher rate of cyber incidents but a significant difference between operational (44%), management (37%) and C-suite (19%) perceptions
- This may be due to a lack of reporting but underlines decision makers don't seem to be aware of the scale of the problem

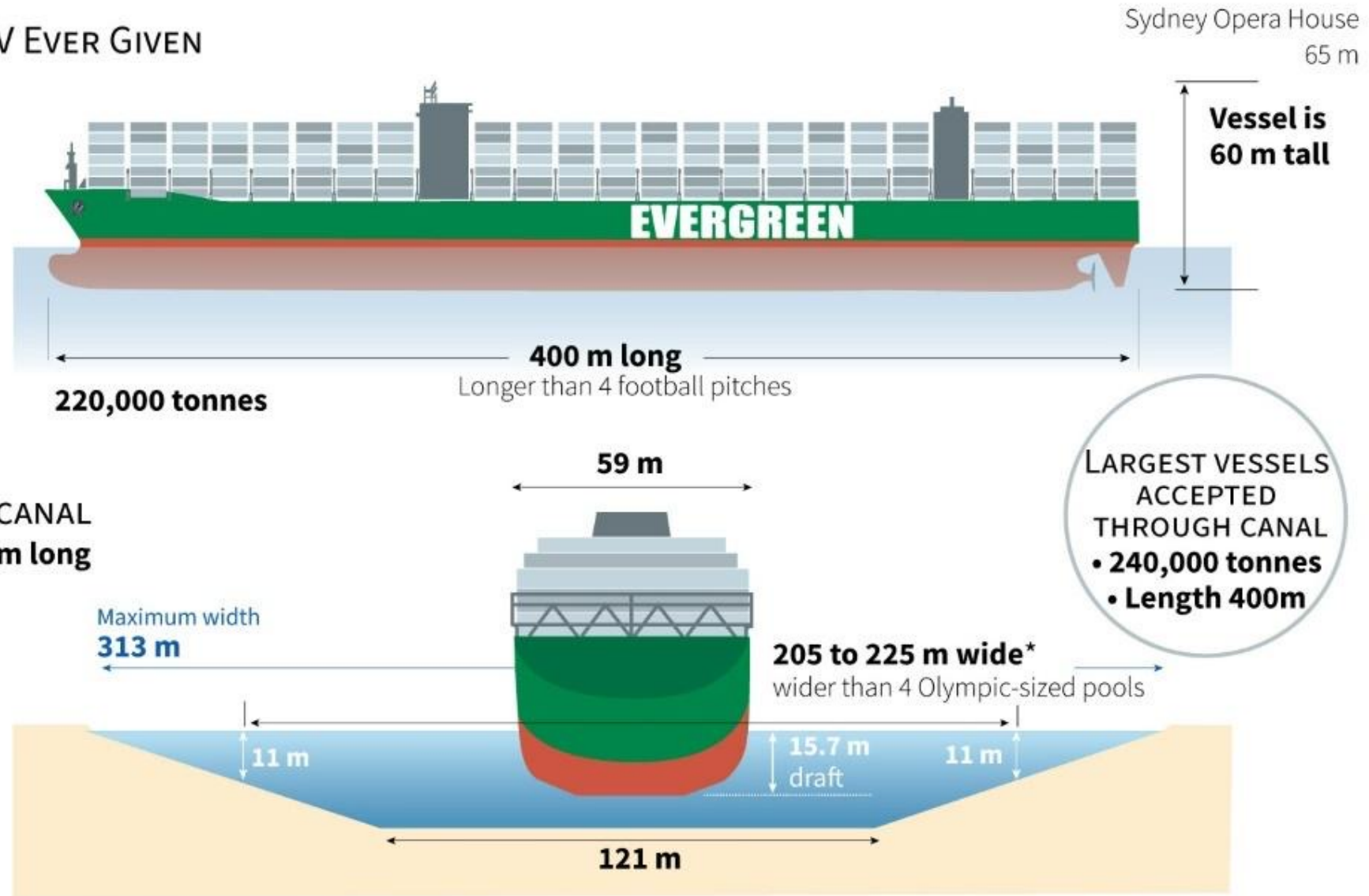




MV Ever Given and the Suez Canal

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

THE MV EVER GIVEN



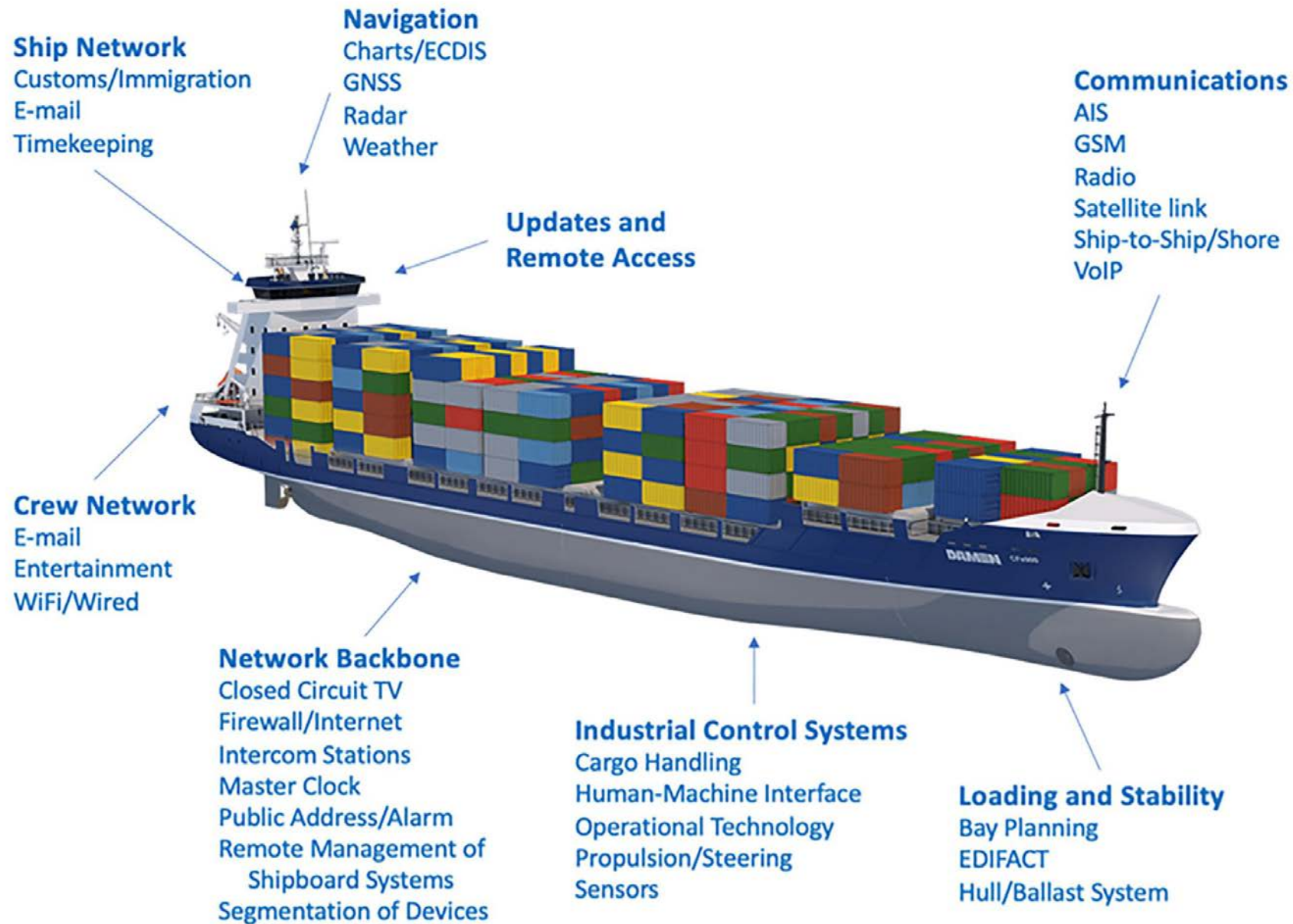


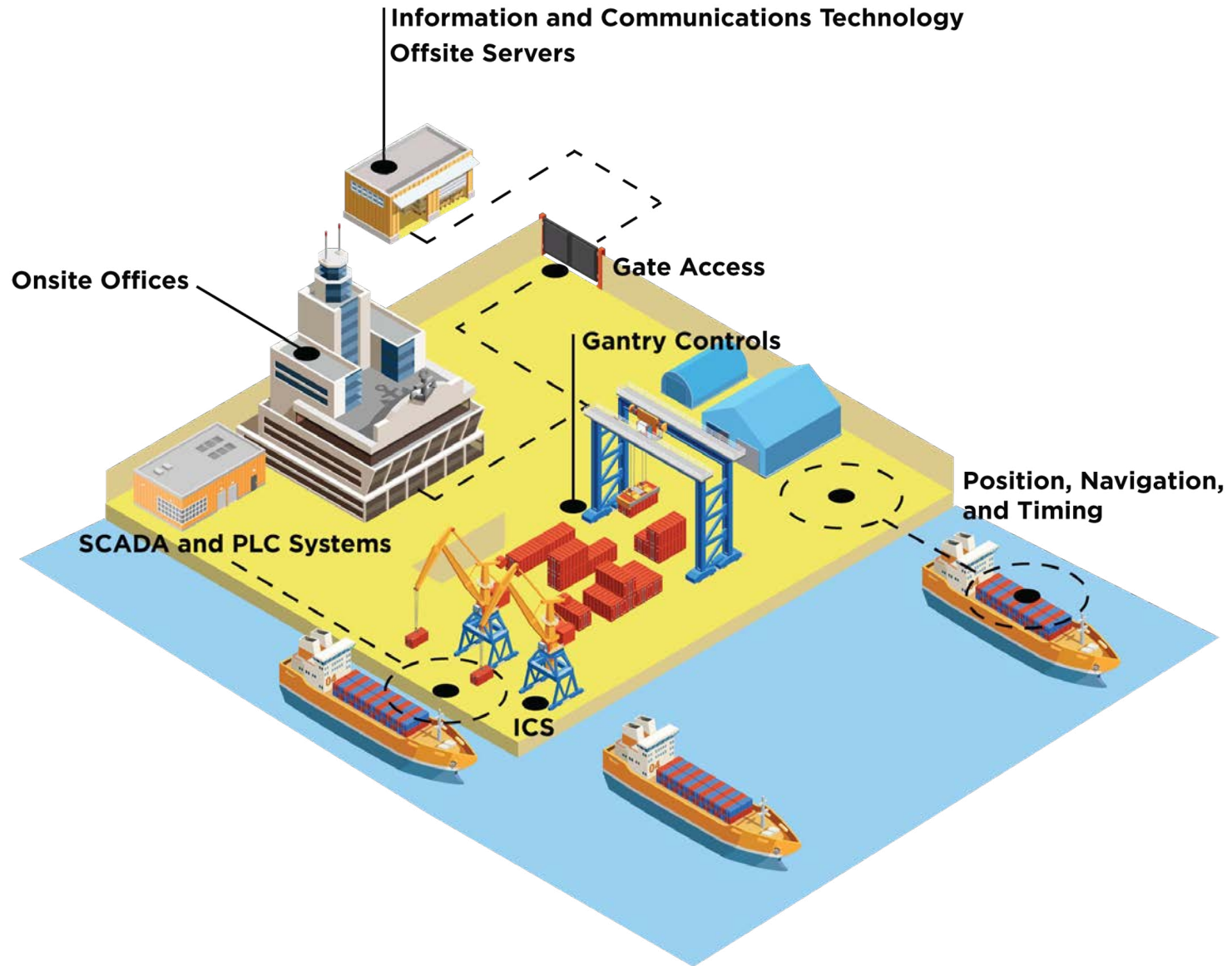
(Kessler and Shepard 2022)

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.



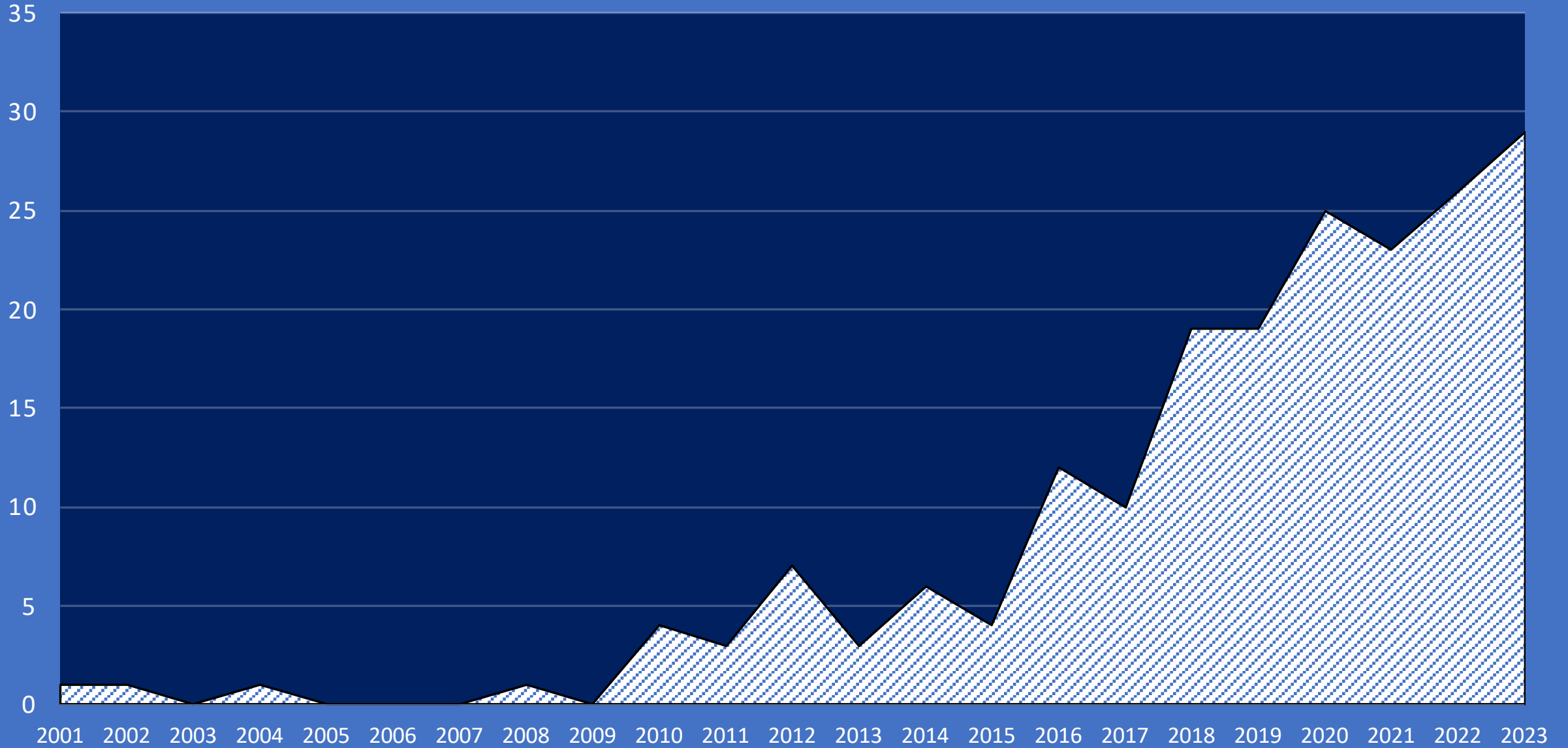


STIX Database

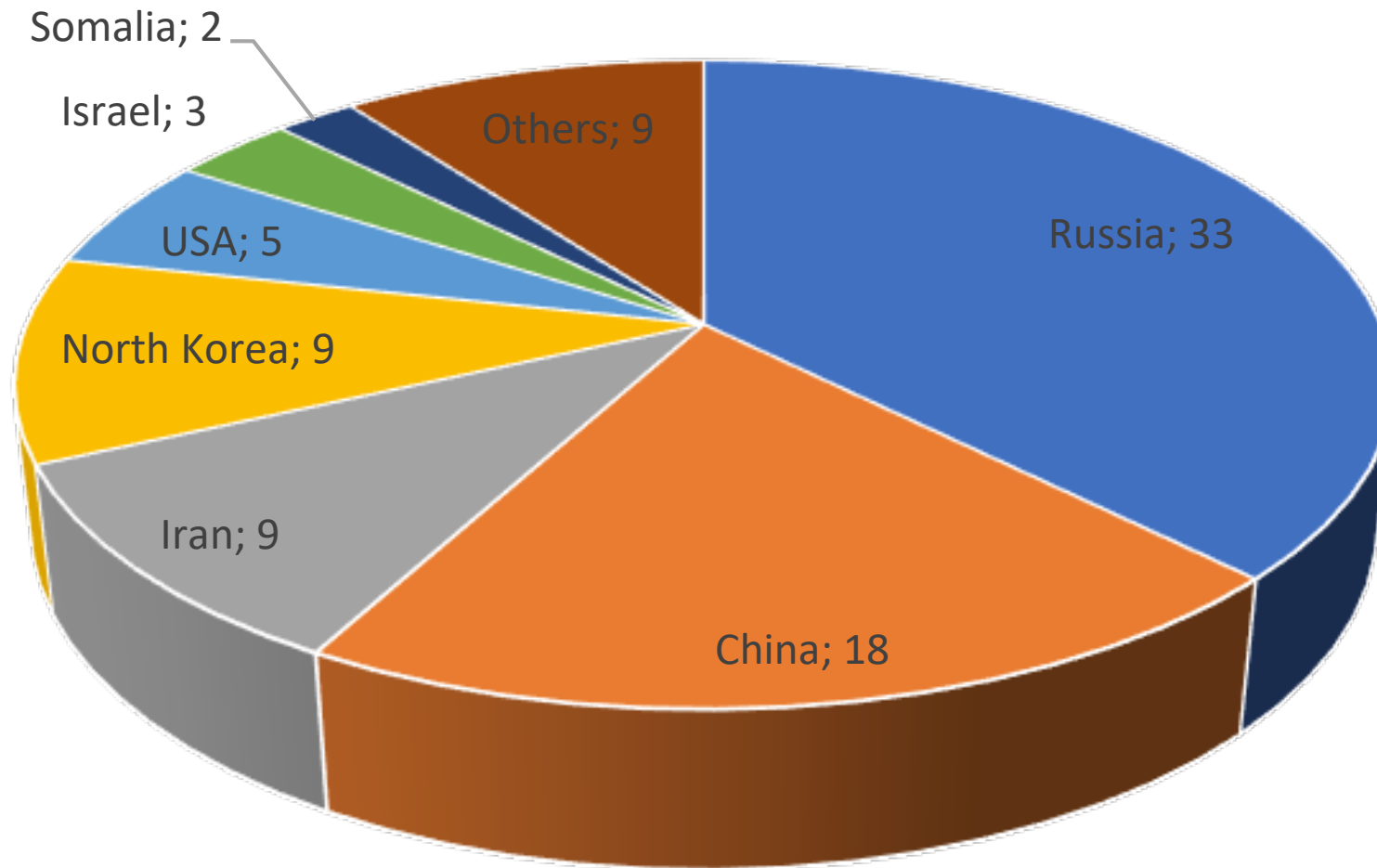
The place for maritime cyber incidents reporting

[Login/Register](#)

Martime Cyber Incidents by Year 2001-2023

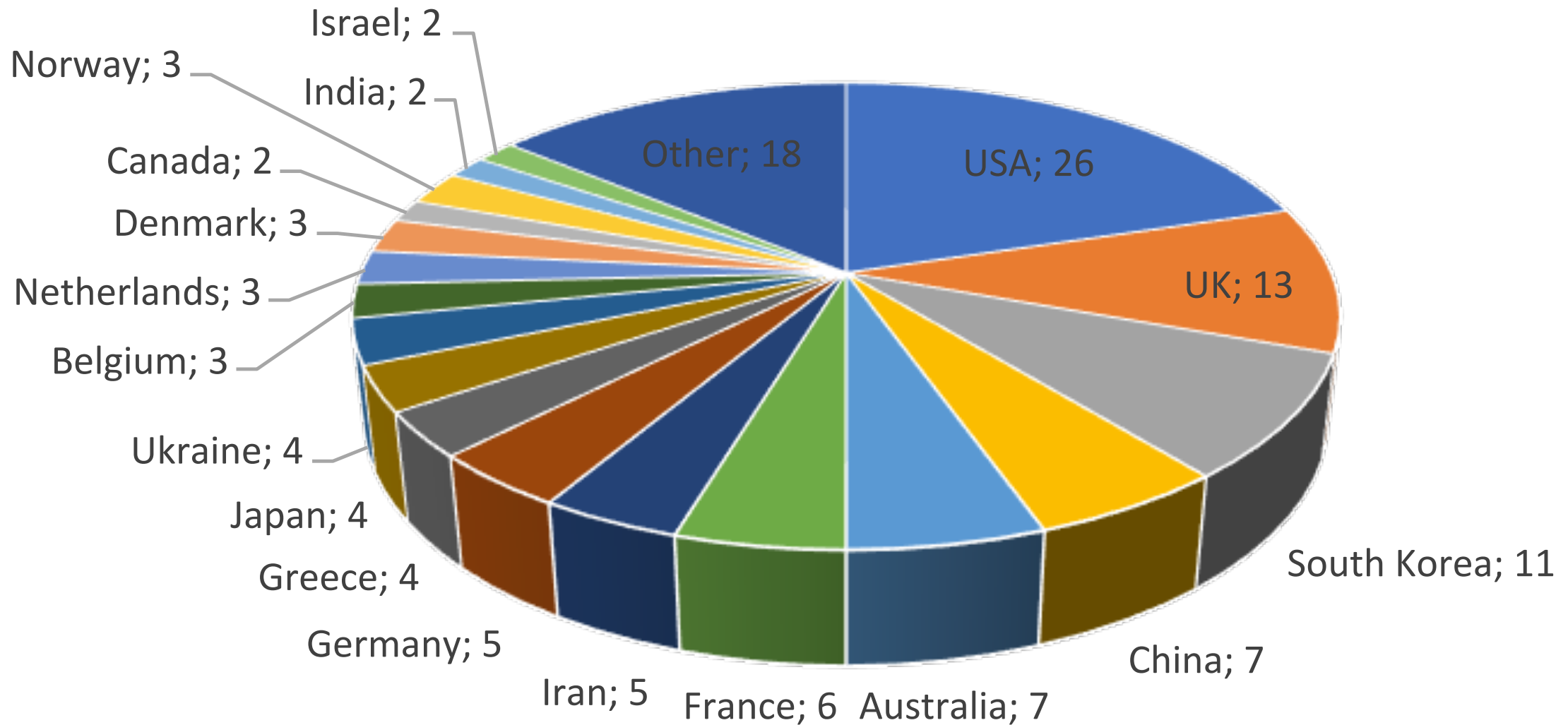


Cyber Incidents by Attacker Country 2001-2022

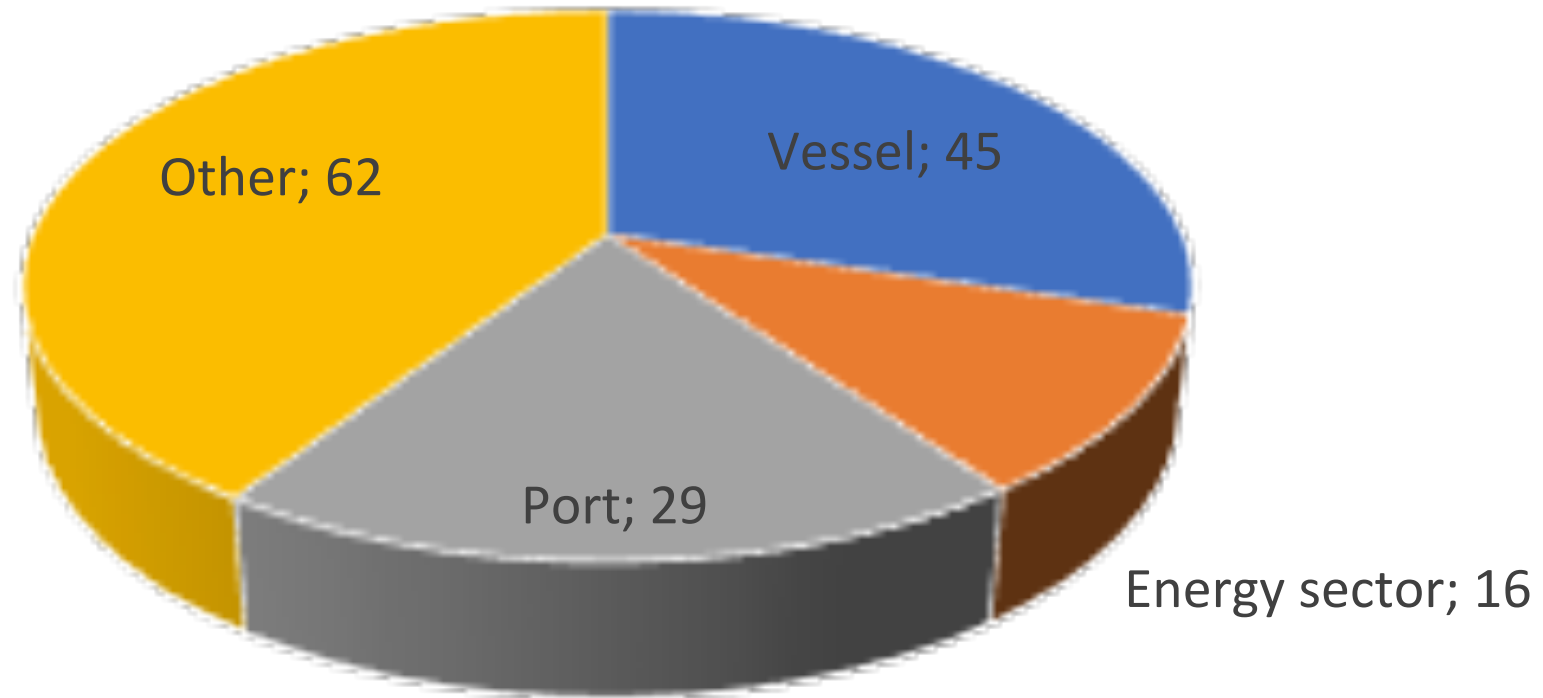


■ Russia ■ China ■ Iran ■ North Korea ■ USA ■ Israel ■ Somalia ■ Others

Maritime Cyber Incidents by Victim Country 2001-2022

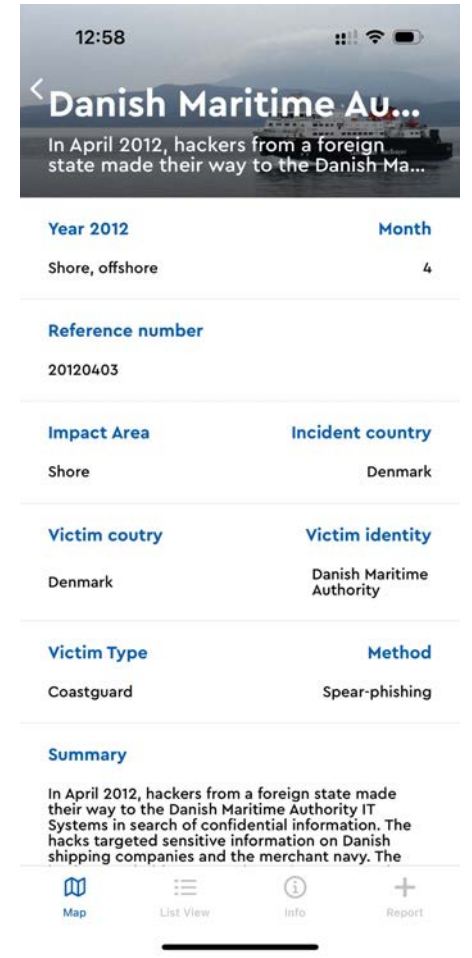
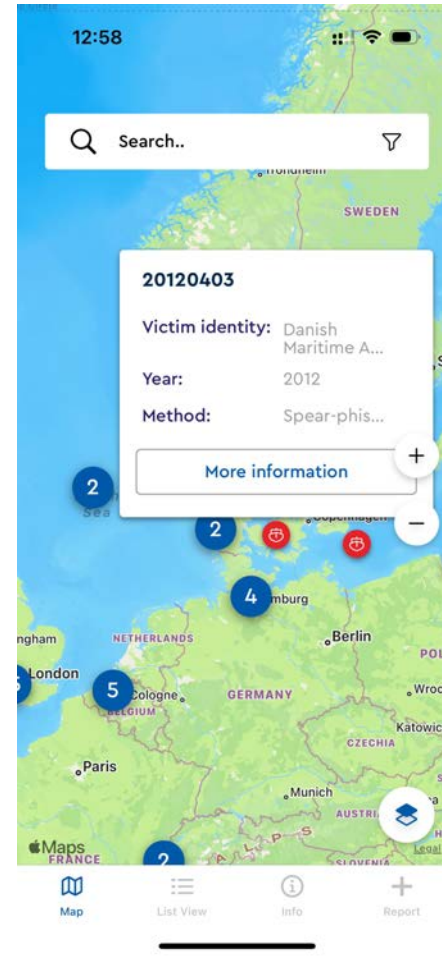
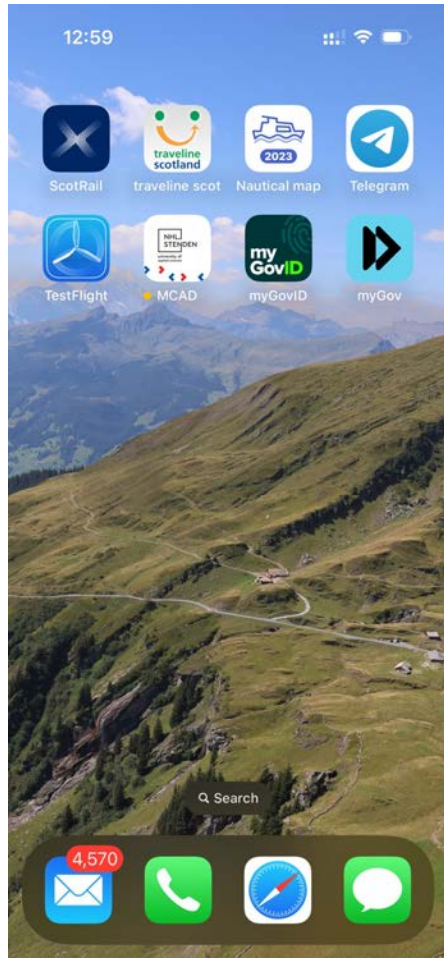


Maritime Cyber Incidents by Victim Type 2001-2022



■ Vessel ■ Energy sector ■ Port ■ Other

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

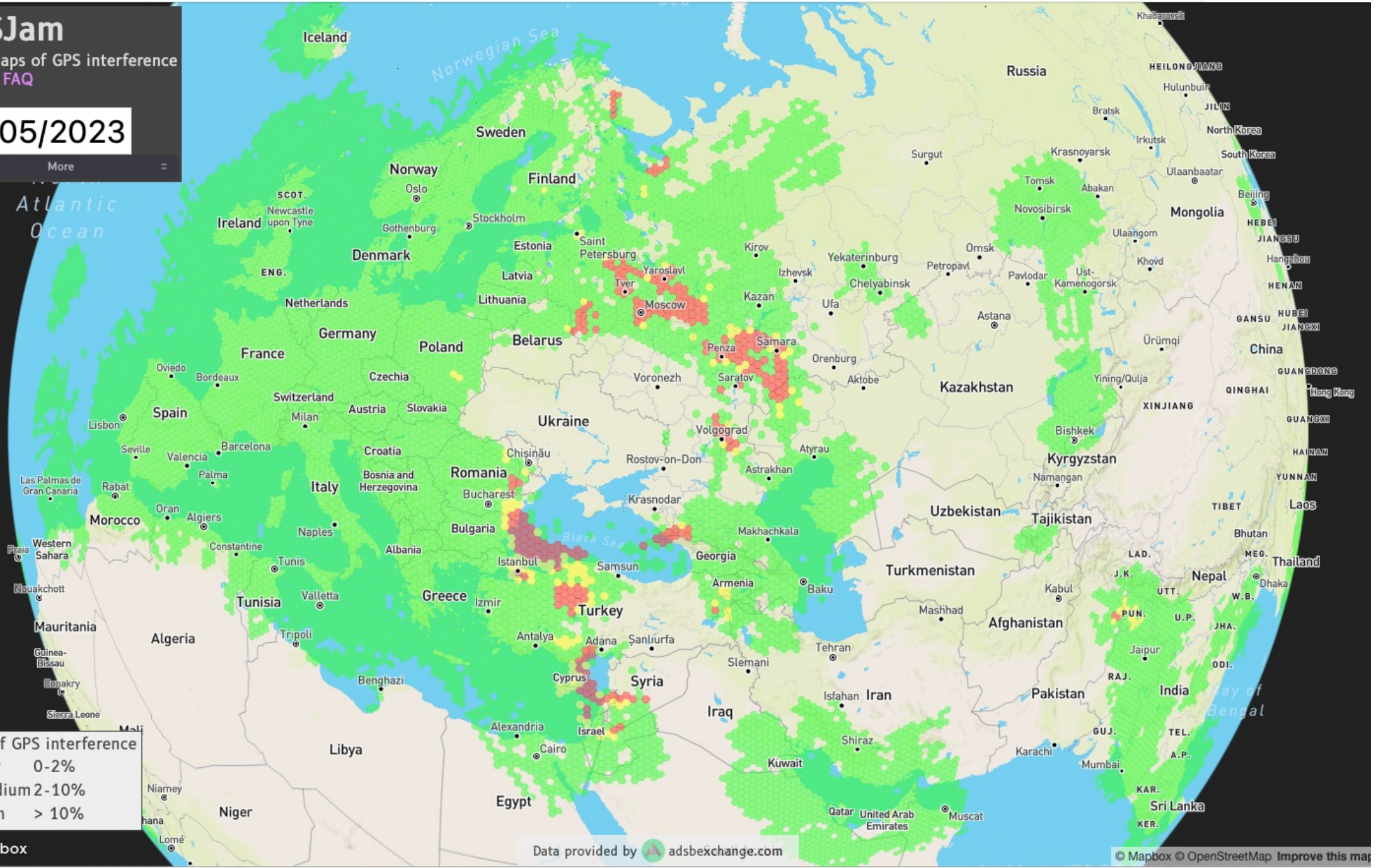
Level of GPS interference

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

mapbox

Data provided by [adsbexchange.com](#)

© Mapbox © OpenStreetMap Improve this map





UNITED STATES COAST GUARD
U.S. Department of Homeland Security

MARINE SAFETY ALERT
Inspections and Compliance Directorate

July 8, 2019
Washington, D.C.

Safety Alert 06-19

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

In February 2019, 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.

Maersk & NotPetya (Selby 2021)

- 20% of global trade and 1/3 of all bananas are shipped by Maersk
- 2016: Maersk IT execs approved and budgeted for network segmentation, but KPIs meant implementation was delayed
- 2017: Maersk admits it had a low-level of cyber maturity
- Maersk Odessa Finance Executive requested M.E. Docs be installed onto their PC
- 27 June 2017: Ukraine's National Constitution Day NotPetya released
- NotPetya took just 7 minutes to take down most of its global network, causing catastrophic damage in less than 1 hour
- Recovery: reached out to suppliers and customers for help; Deloitte sent 200 workers to Maidenhead UK; 1 (of 150) surviving Active Directory server flown from Nigeria; Maersk bought & built 2000 laptops from scratch in 6 days
- Non-global applications which supported local processes were the hardest to recover

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

    1Mz7153HMuxXTuR2R1t78mGSdzaftNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail
    wowsmith123456@posteo.net. Your personal installation key:

    [REDACTED]

If you already purchased your key, please enter it below.
Key: _
```

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"



(U) M/V MERCER STREET (Stock Photo)



(U) Damage Caused by Iranian UAV Attack



(U) Debris From Failed Iranian UAV Attack



(U) Iranian UAV Impact Location

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...'

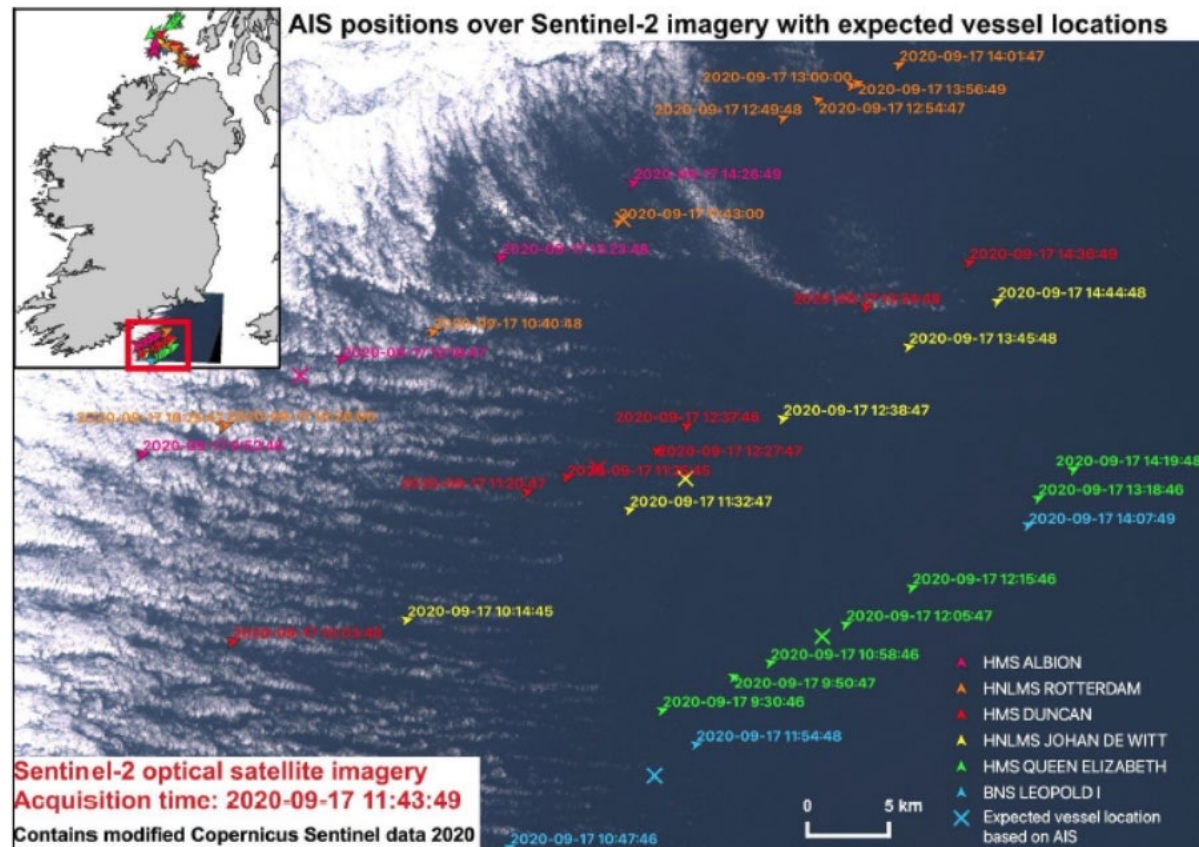


Saving money using cryptocurrency swaps

Ziggo zakelijk

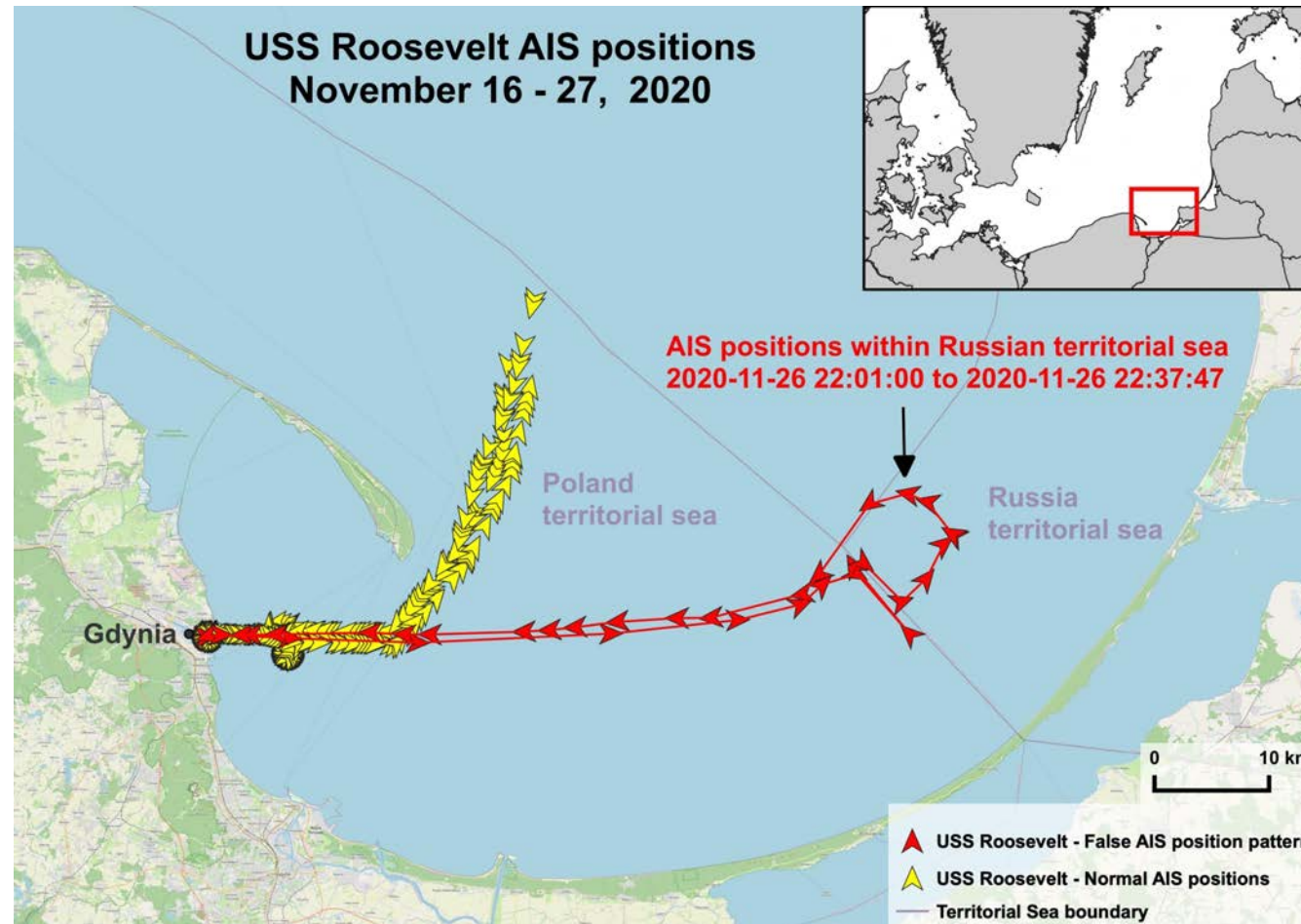
2 maanden Gratis

AIS spoofing (skytruth.org 2021)

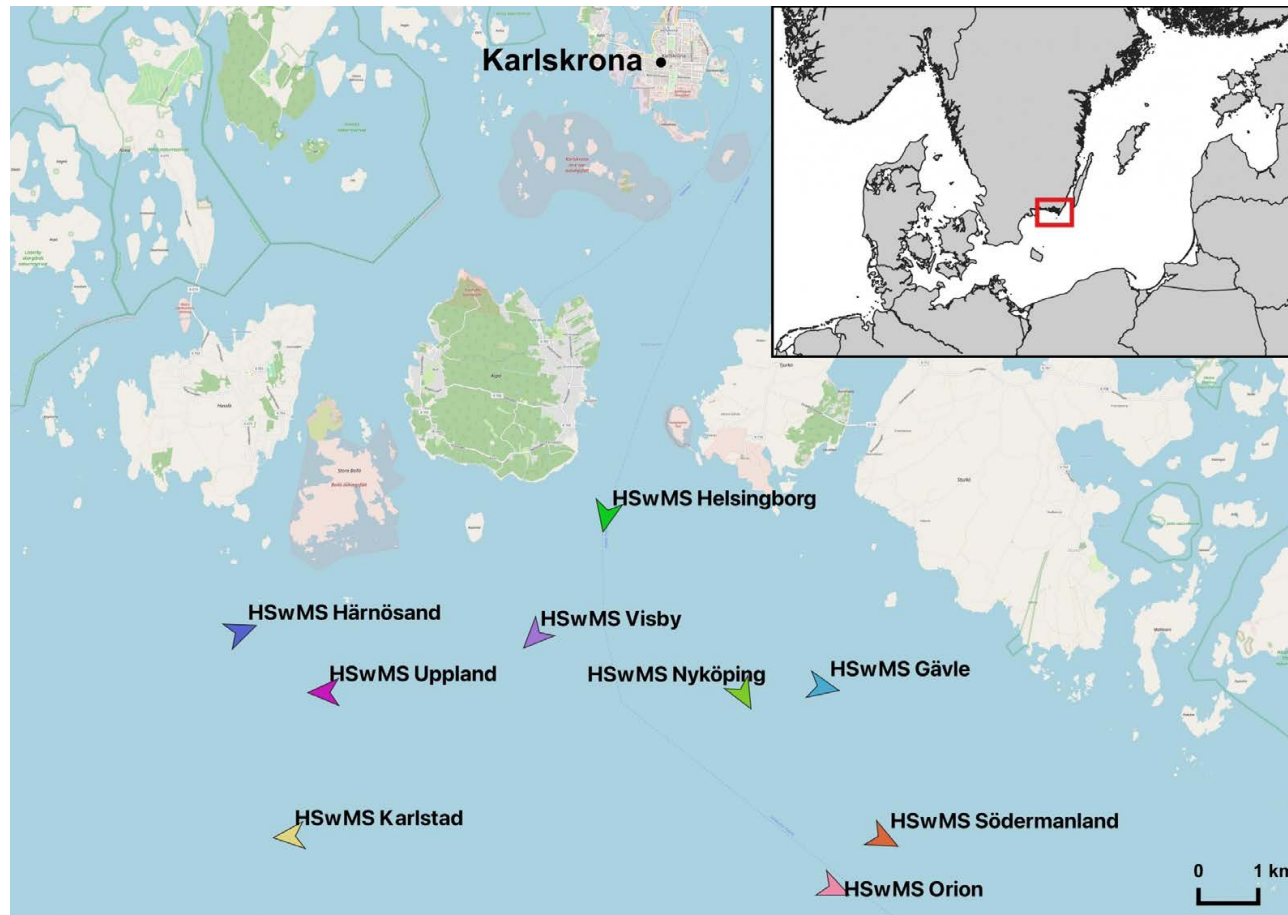


False AIS tracks of six naval vessels from the United Kingdom, the Netherlands, and Belgium overlaid on a S2 satellite image of the same day, revealing that none of the vessels were actually present at the time of S2 image acquisition. Image copyright SkyTruth and Global Fishing Watch 2021. AIS data courtesy of Global Fishing Watch/Orbcomm/Spire.

AIS spoofing (skytruth.org 2020)



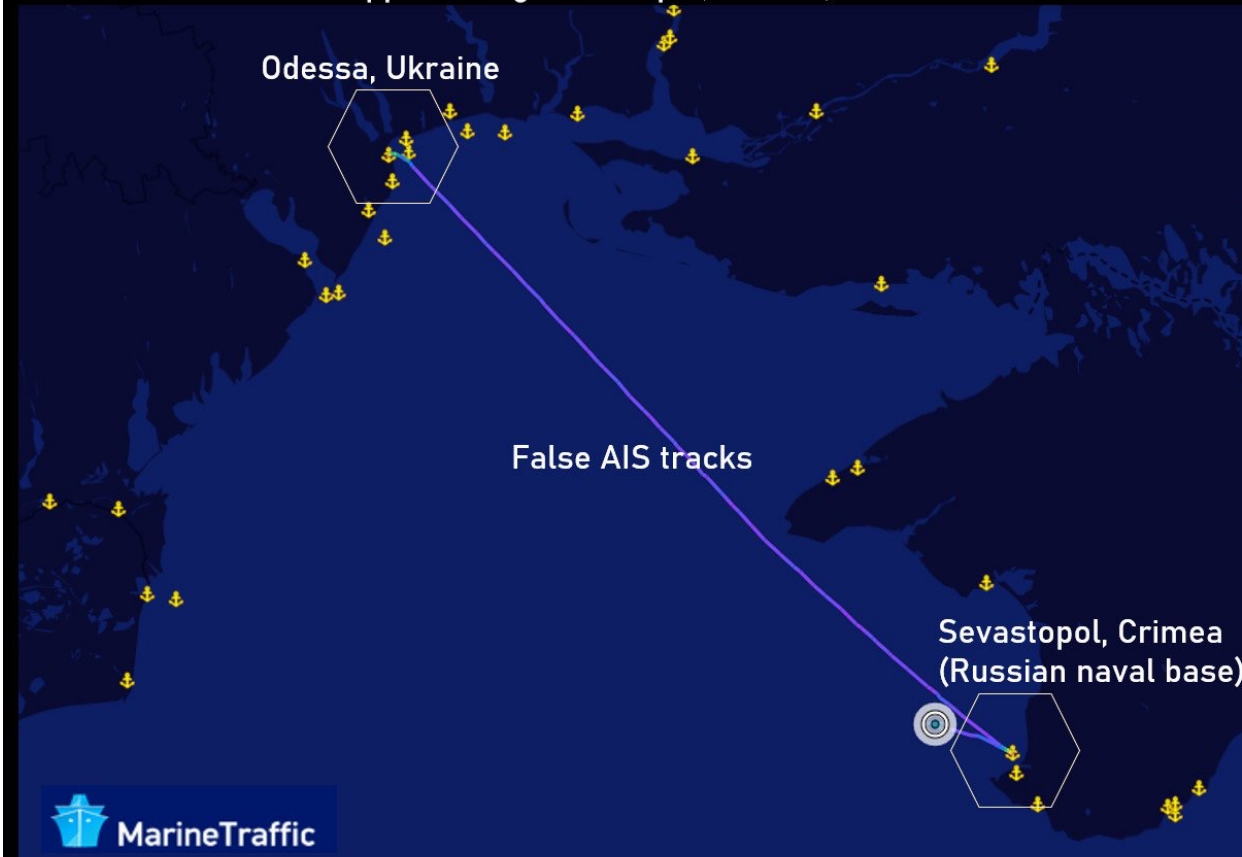
AIS spoofing (skytruth.org 2020)





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.



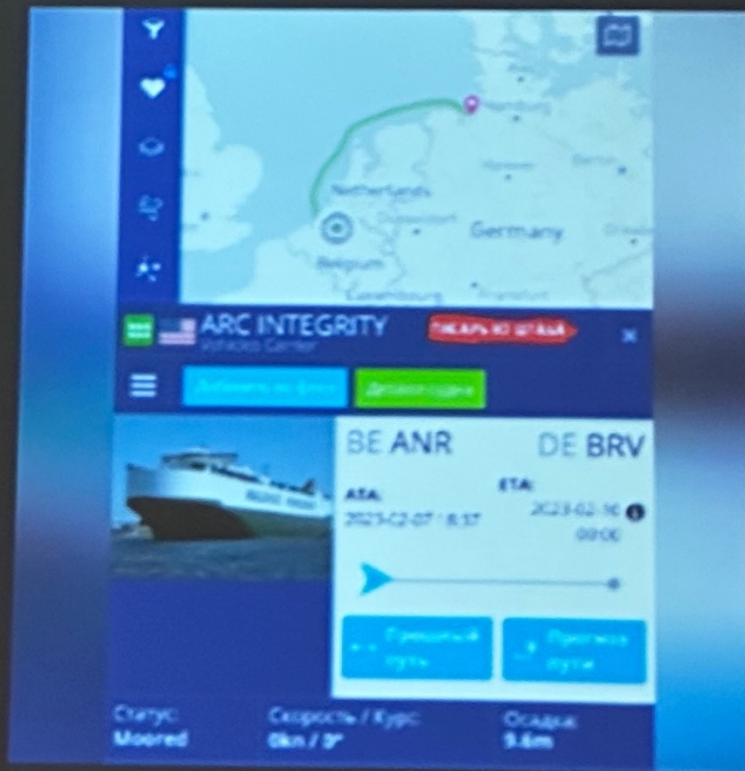


KILLNET CHAT

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

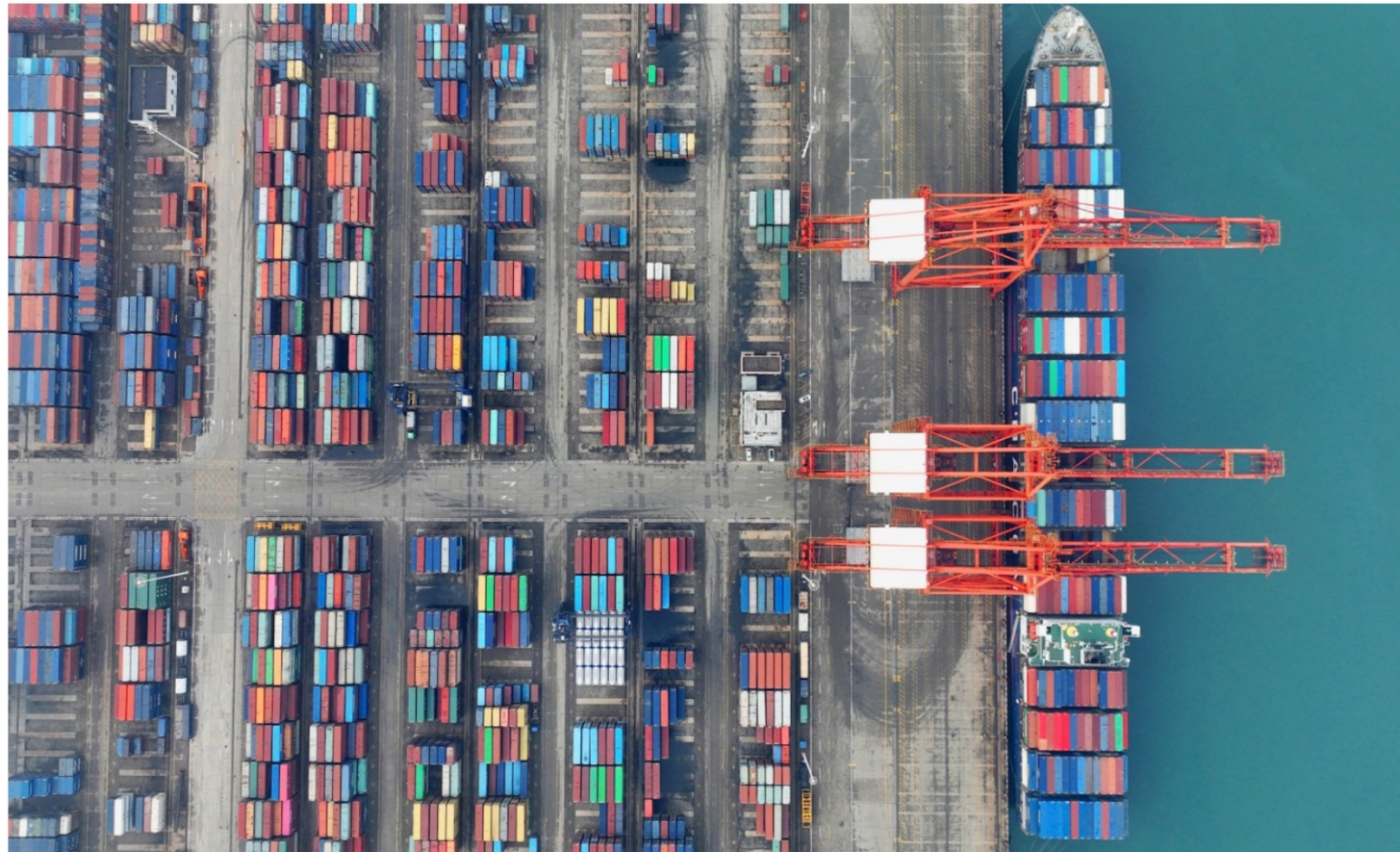


 Image Credits: STR / AFP / Getty Images

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.

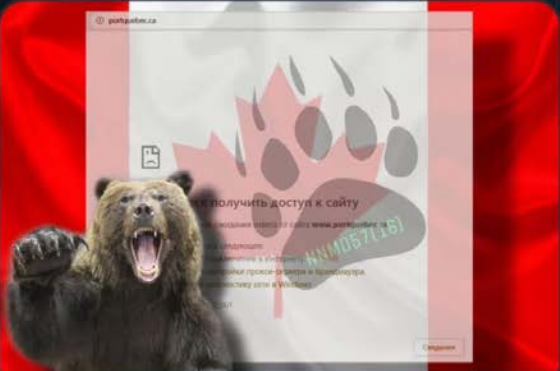
1:44 M LS P • 📶 🔋

←  **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



Pirates use of Technology (2011)

(<https://www.nbcnews.com>)

- These days, pirates off the Horn of Africa are turning to a sophisticated mix of weaponry, jury-rigged GPS devices and ingenious hacks of shipping-industry databases to hunt down prey. Andrew Mwangura of the East African Seafarers Assistance Program detailed the methods used by the pirates:

"The most important thing for Somali pirates is getting relevant information regarding merchant vessels that they wish to hijack. But this does not come easily without the use of certain technologies [...] What they must know includes information on the value of vessels, the value of the goods and the number of crew members [...] They use navigational technologies in their daily operation. This involves a combination of technologies, most important[ly] they use satellite cell phones for long range communications."

Oil Tanker Cyber Attack (2014)

<https://safety4sea.com/>



- In January 2014 the ship MT Kerala was hijacked and went dark in Angola and Nigeria after Pirates disabled the vessel's AIS and other communication equipment so that the vessel could not be tracked from shore or satellite and painted over the identifying features of the vessel, including stack, name and IMO number.
- The consequence of the attack was that \$10 million of Cargo (oil) was stolen via ship-to-ship transfer. They undertook three separate ship-to-ship transfers of cargo amounting to the theft of approximately 12,271.5 tonnes of cargo.
- The hijacking of the Dynacom Tanker in an area where a known suspect vessel was operating was an embarrassment for the Angolan Navy.
- During the hijacking, one crew member was stabbed by the pirates and others were beaten.



Cyber Aided Cargo Theft (Verizon DBIR 2016)

- In 2016, an Shipping Company was hit by a hacking attack.
- The hackers, swashbuckling criminals, pirates, gained access by hacking the content management system of the company (CMS).
- The pirates hacked into the systems in order to get a sneak preview of the cargo.
- They uploaded a malicious web shell onto a server running the company's CMS.
- The pirates used this compromised system to view key shipping and inventory data, including bills of lading. After that, they searched by bar code for highly valuable items.
- They wanted to be able to attack the ship efficiently by locating the exact vessel and cargo containers they wanted to plunder.
- It resulted in valuable cargo theft.



Navigation System Compromise

(Fairplay 2017)

- In February 2017 hackers reportedly took control of the navigation systems of a German-owned 8,250 teu container vessel en route from Cyprus to Djibouti for 10 hours.
- “Suddenly the captain could not manoeuvre,” an industry source who did not wish to be identified told Fairplay sister title Safety At Sea (SAS). “The IT system of the vessel was completely hacked.”
- There are three German shipowners that operate eight vessels between 8,200 and 8,300 teu, according to IHS Markit data, one of which confirmed knowledge of the attack to SAS but denied it was a vessel from their own company.
- While details are limited, according to the source, the 10-hour attack was carried out by “pirates” who gained full control of the vessel’s navigation system intending to steer it to an area where they could board and take over. The crew attempted to regain control of the navigation system but had to bring IT experts on board, who eventually managed to get them running again after hours of work.

Seized UK tanker likely 'spoofed' by Iran

GPS spoofing involves ships' receivers being tricked with counterfeit satellite automatic identification signals generated to gain control of a navigation system. This can take the vessel off course or show it in a different location

16 Aug 2019 | NEWS |



by [Michelle Wiese Bockmann](#)

[@Michellw_](#)

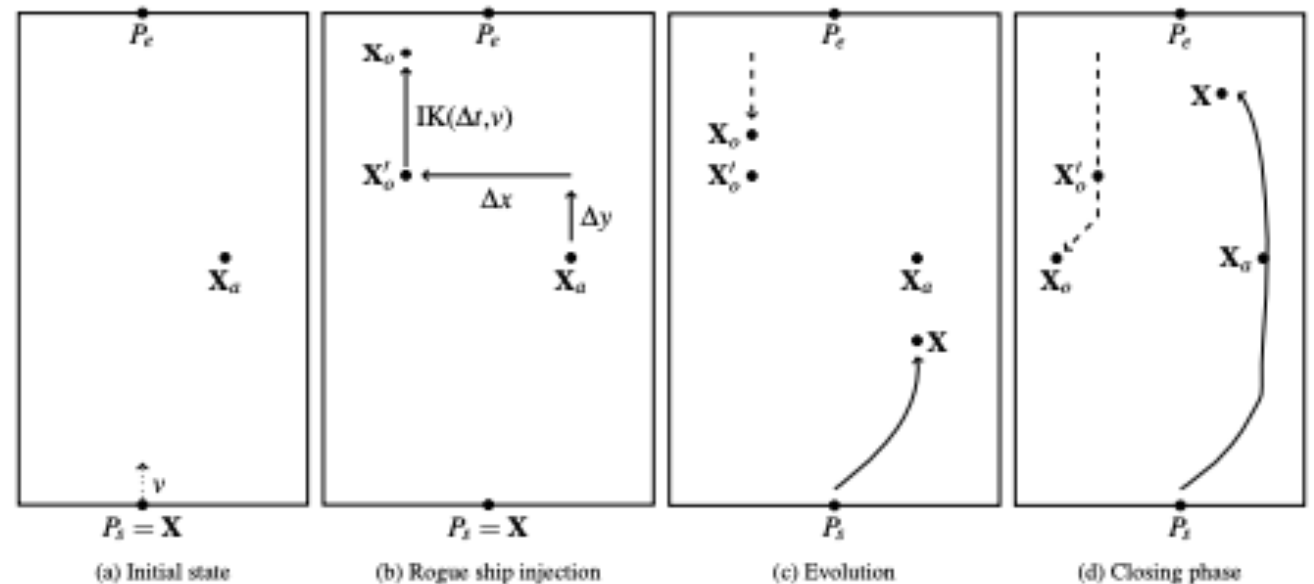
michelle.bockmann@loydslistintelligence.com

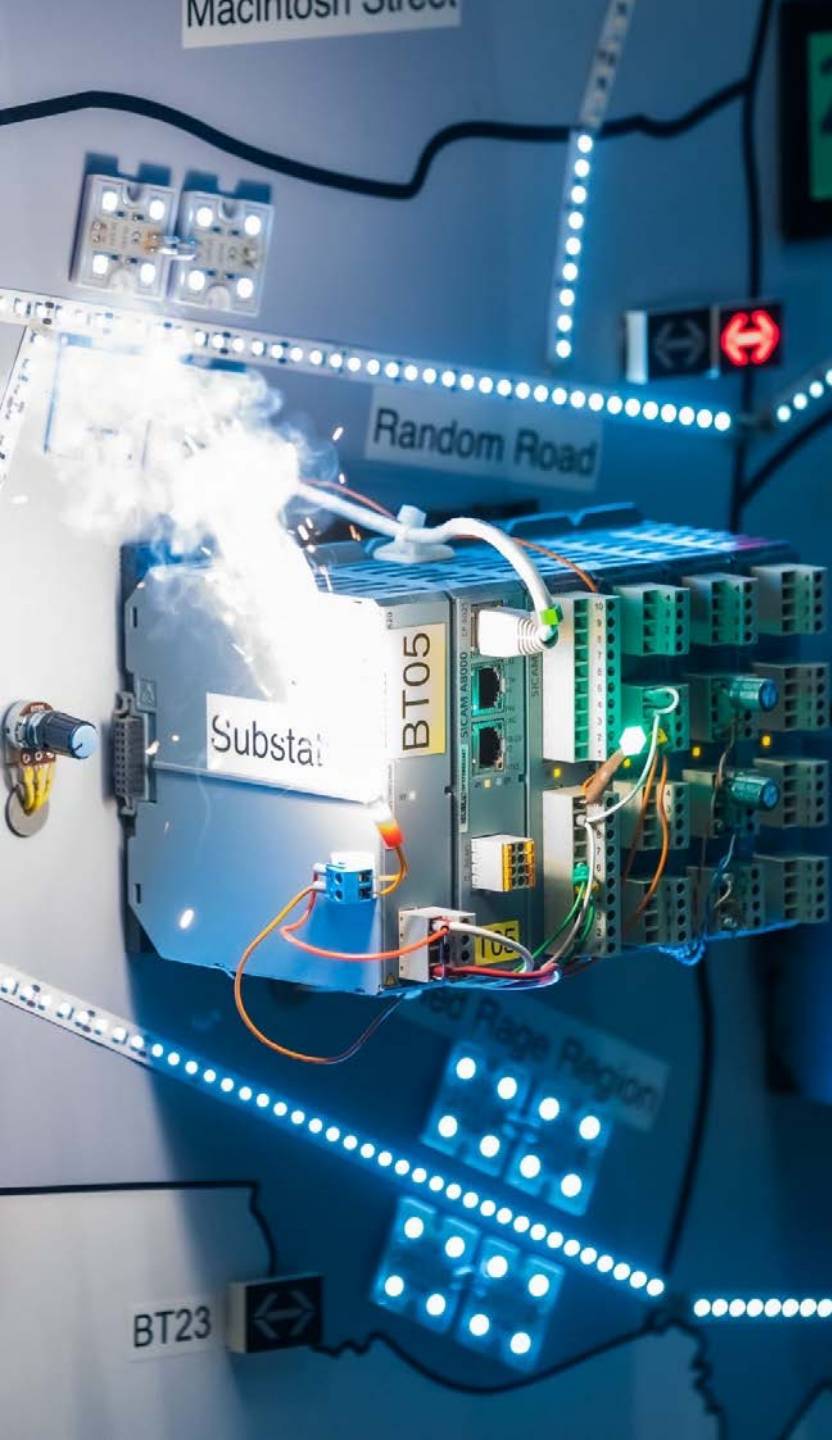
Analysis of AIS data by Lloyd's List Intelligence shows for the first time that Stena Impero fitted the pattern for a spoofing attack when it was seized by the Islamic Revolutionary Guard Corps on July 19



Collision-avoidance cyber-attack to the navigation sensors (Longo 2023)

- Thinking of the future, many cyber-attack scenarios might involve autonomous ships: for instance, an autonomous ship might be lured near a fixed threat such as minefields, or in an area that exposes it to other threats, such as collisions or grounding.
- Moreover, thinking about future piracy, the ship could be forced to steer in a dangerous area to be seized to obtain a ransom.
- The attacker can also unnecessarily lengthen a trip to damage goods or make them arrive late.
- Lastly, a ship can be forced to bypass the territorial sea or navigate in off-limit areas.
- All these possible scenarios can have severe consequences, and the near-future automation designers should face with.



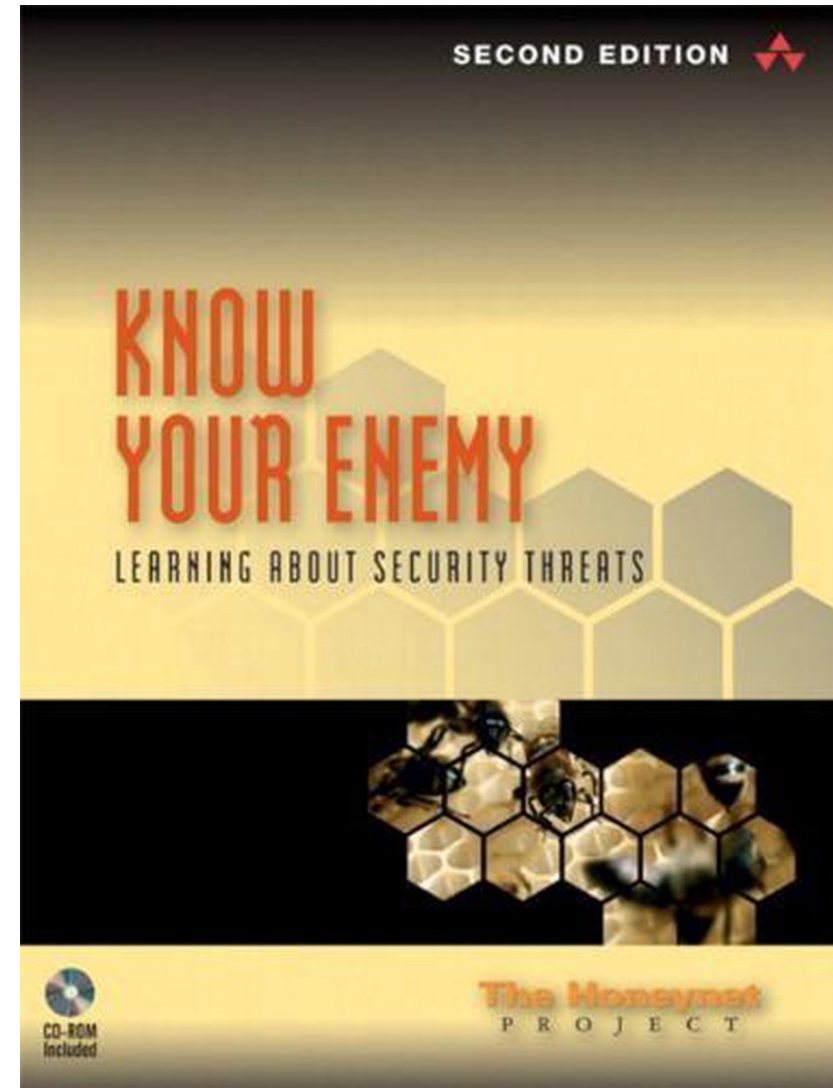


Create Maritime Technology Hacking Lab

- 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

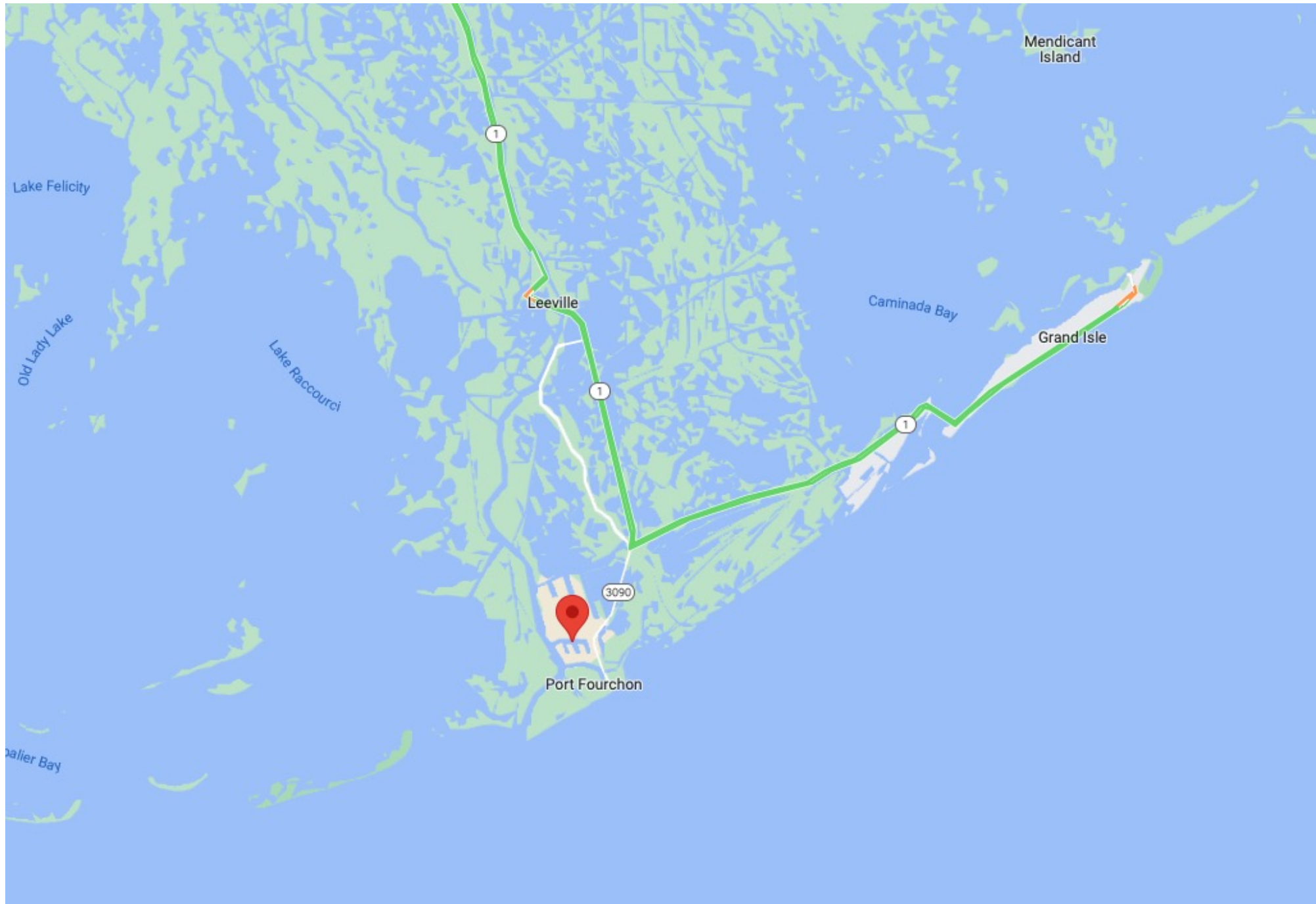
Modem: GMXP:
 Net Power
 Tx Status
 Rx1 ADU power
 Rx2 CM power
 Status

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

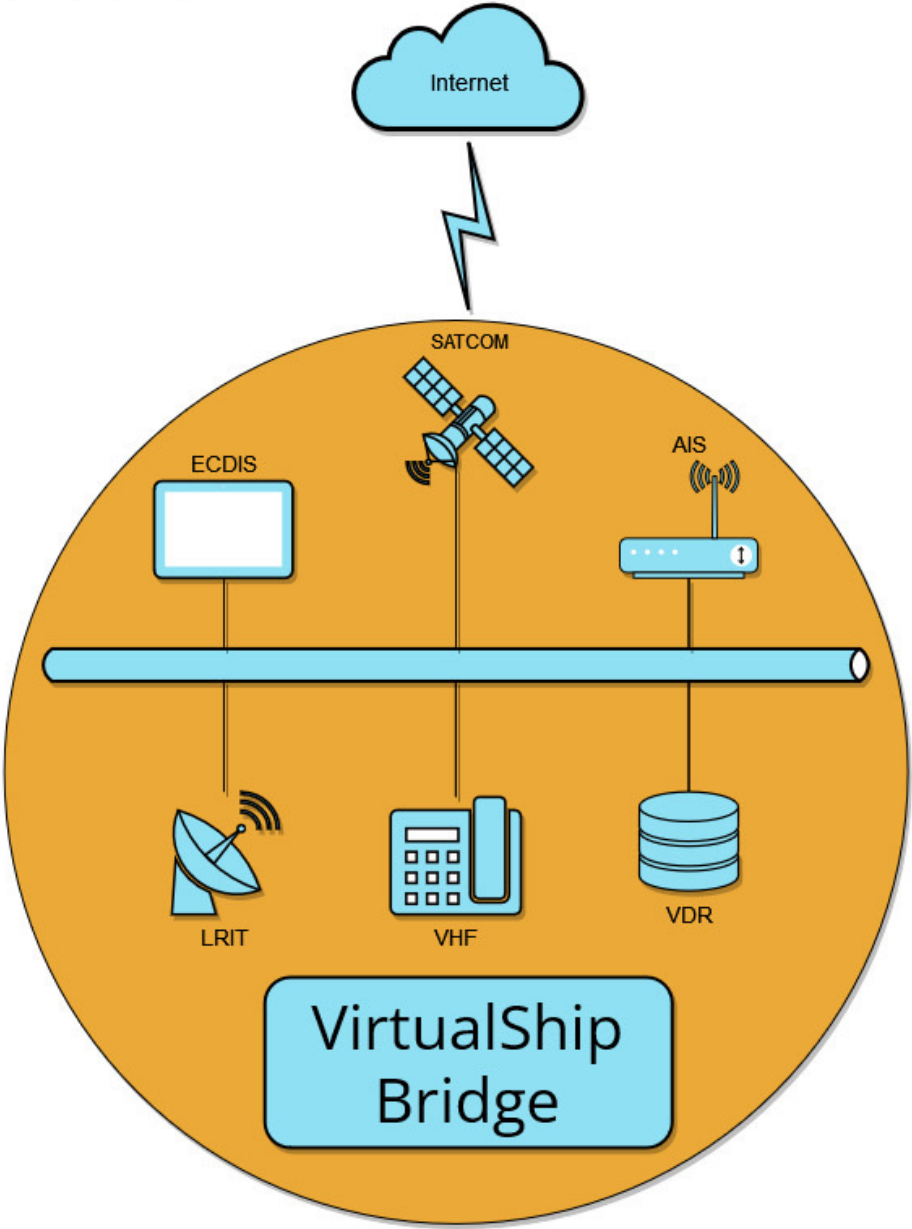
Palier Bay

1

1

1

3090



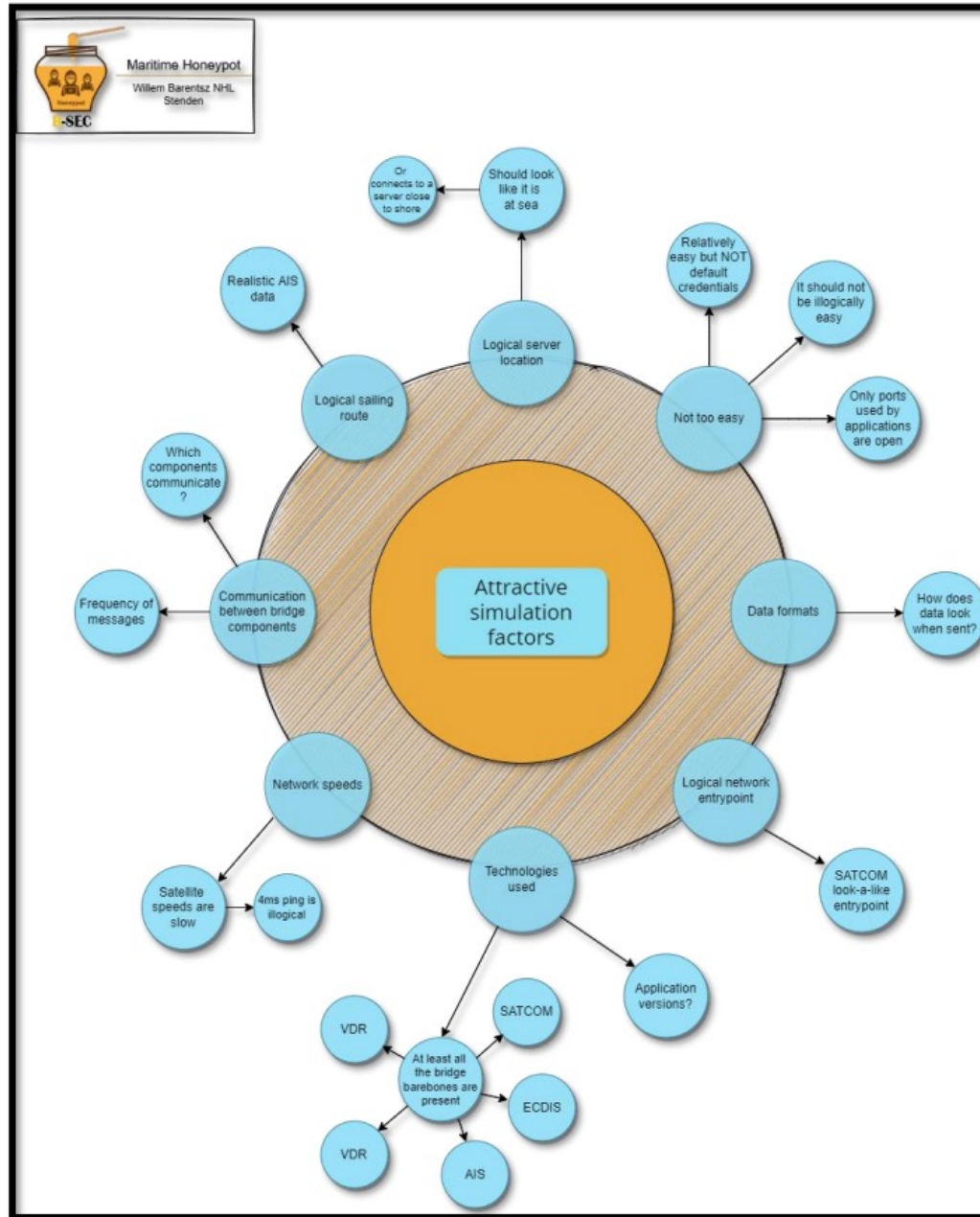


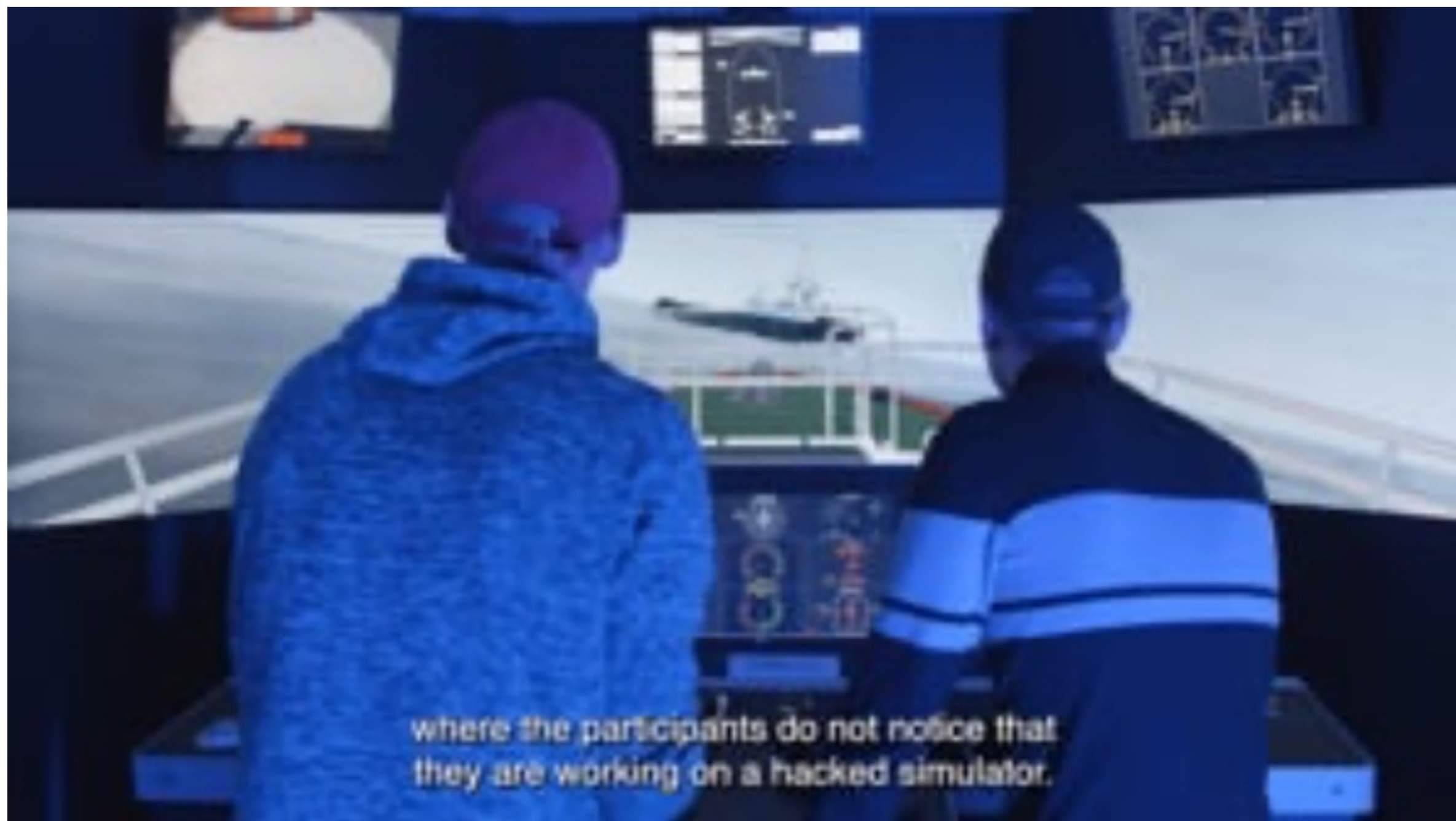
Figure 4 – Mindmap attractive simulation factors.



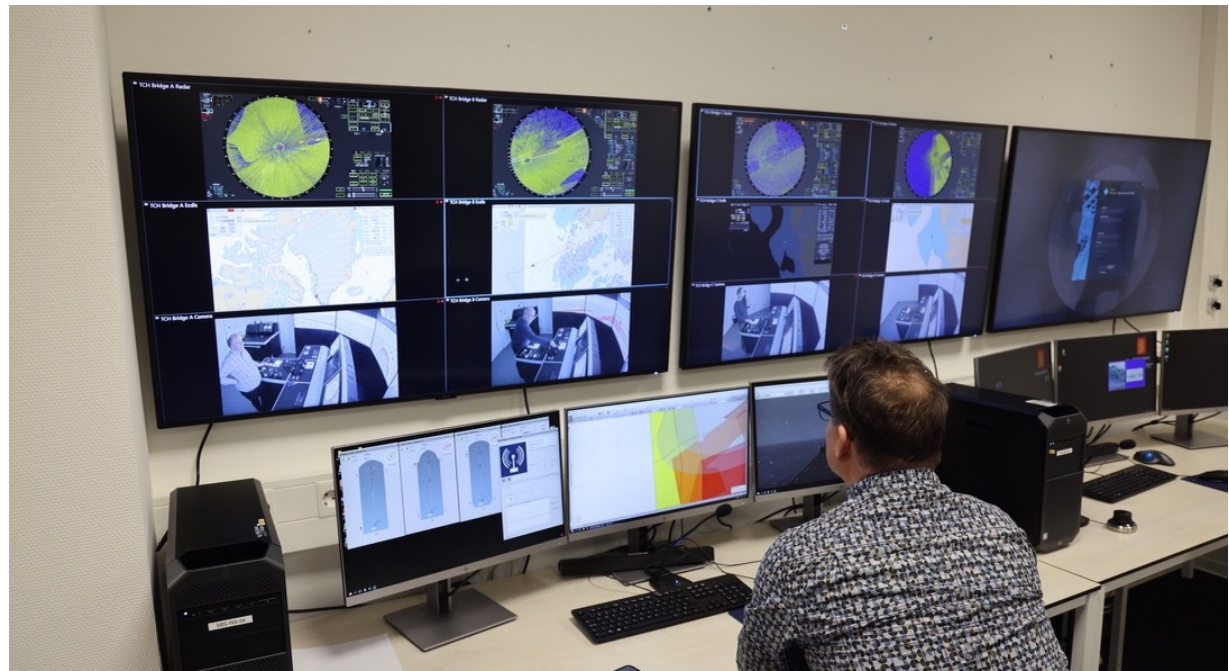
Maritime Cyber Incident Simulations

- 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

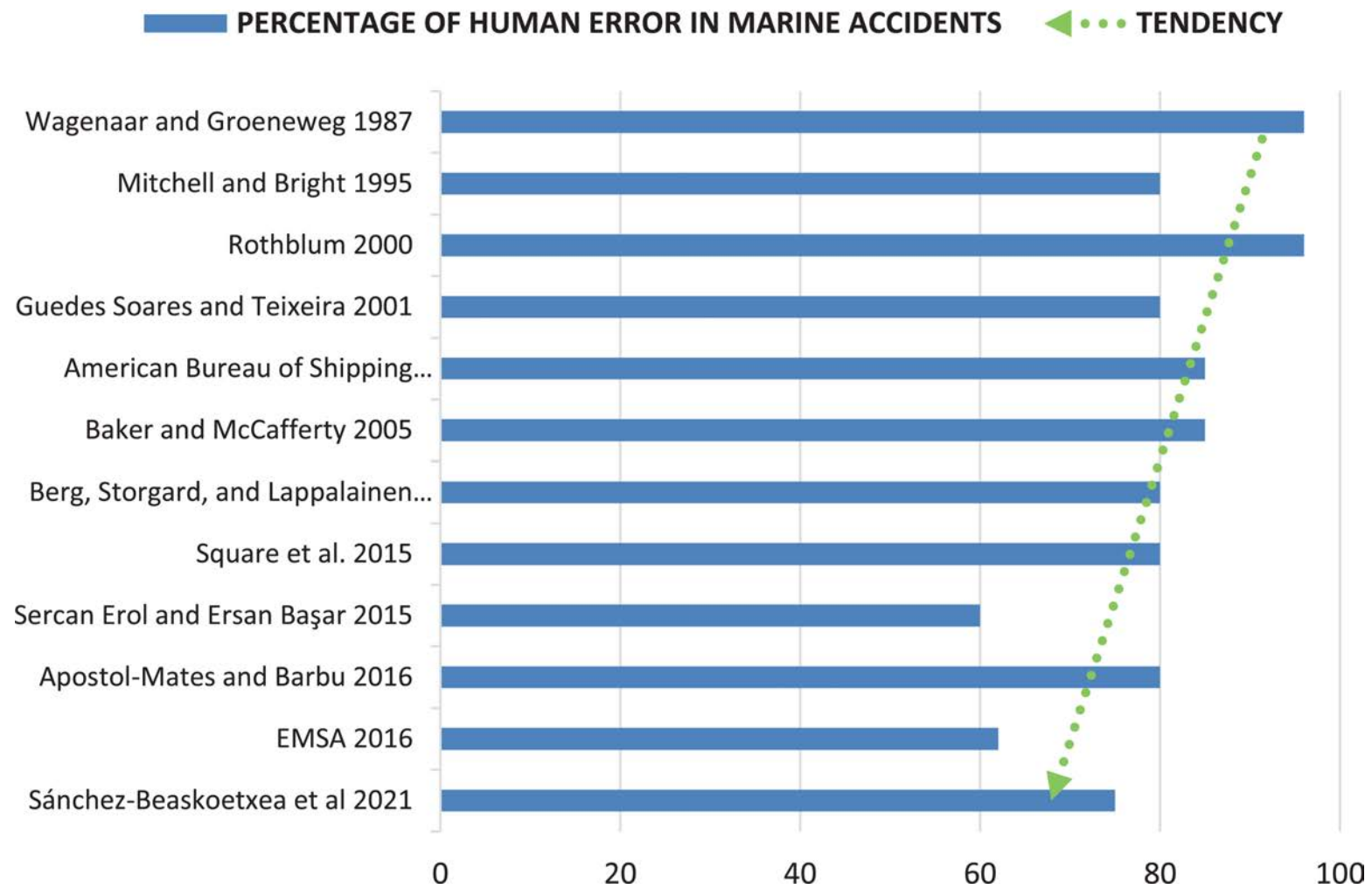
10:04 PM · Aug 21, 2017

1.2K Reply Share

[Read 118 replies](#)

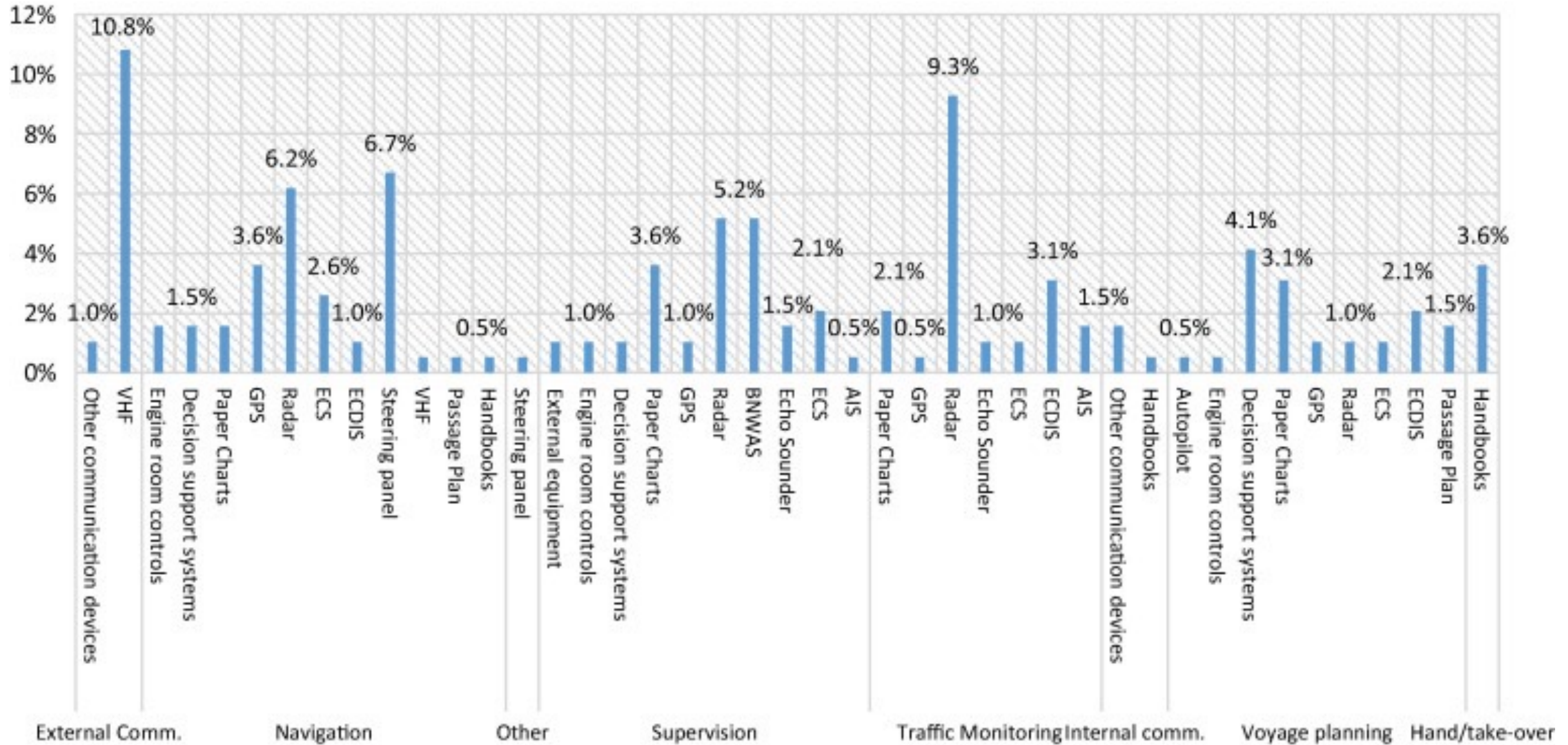


Percentage of human error in marine accidents according to several authors.



Javier Sánchez-Beaskoetxea et al 2021

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



Current Cyber Threats to Maritime Security

Webinar – 13th April 2022

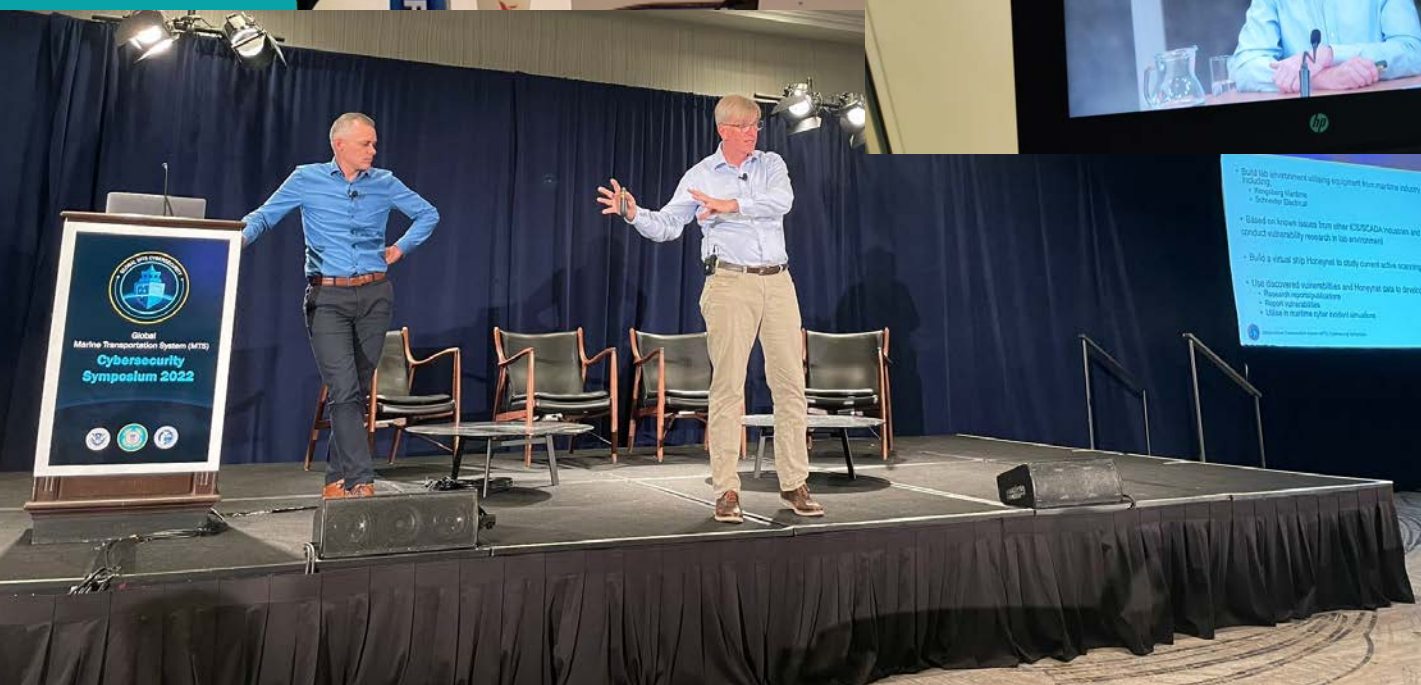
NHL
STENDEN

university of
applied sciences



NHL
STENDEN

hogeschool



- Build the environment using equipment from maritime industry:
 - 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
 - Ideas to improve cyber control interface



OTV
News Flash

Port of Orangeland Cyber-attack

Questions



university of
applied sciences