Maritime Cybersecurity Exercises

Bastiaan Maltha
Stephen McCombie
Jeroen Pijpker

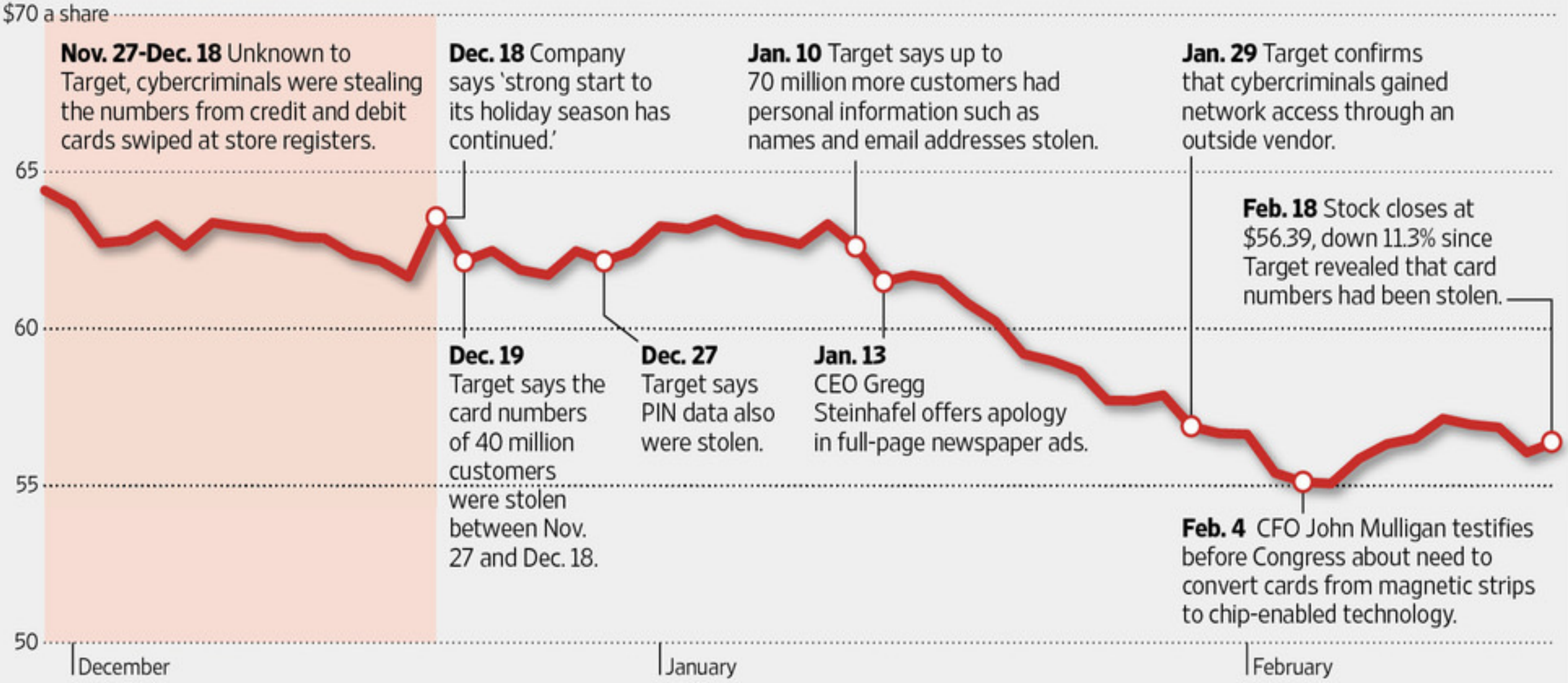
NHL STENDEN
university of
applied sciences

Value of Cybersecurity Exercises

- You need to exercise regularly
- You can run exercises varying in scope, participants and duration
- They help participants understand response processes and their roles in them
- They identify problems in a safe environment where they can be remedied before being needed

Trying Times

Target's discovery that cybercriminals had stolen the credit and debit card numbers of about 40 million customers led to a series of difficult decisions.



Nov. 27-Dec. 18 Unknown to Target, cybercriminals were stealing the numbers from credit and debit cards swiped at store registers.

Dec. 18 Company says 'strong start to its holiday season has continued.'

Jan. 10 Target says up to 70 million more customers had personal information such as names and email addresses stolen.

Jan. 29 Target confirms that cybercriminals gained network access through an outside vendor.

Feb. 18 Stock closes at $56.39, down 11.3% since Target revealed that card numbers had been stolen.

Dec. 19 Target says the card numbers of 40 million customers were stolen between Nov. 27 and Dec. 18.

Dec. 27 Target says PIN data also were stolen.

Jan. 13 CEO Gregg Steinhafel offers apology in full-page newspaper ads.

Feb. 4 CFO John Mulligan testifies before Congress about need to convert cards from magnetic strips to chip-enabled technology.

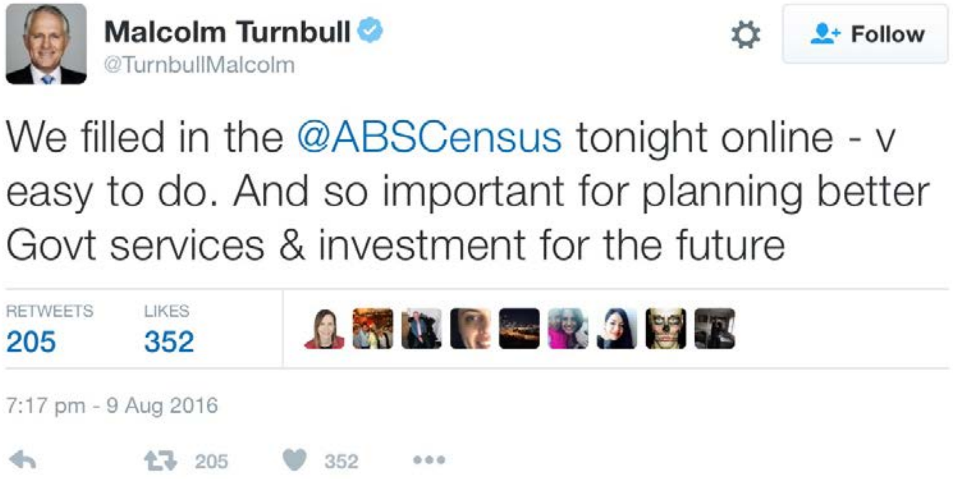
Sources: WSJ Market Data Group; news reports

The Wall Street Journal

Office of Personnel Management 2015

Australian Census August 2016

- On 9 August Australia conducted an online census
- Our tech savvy Prime Minister even tweeted how easy it was
- Things did not go to plan
- It's another example of how you respond during and after a cyber incident is key



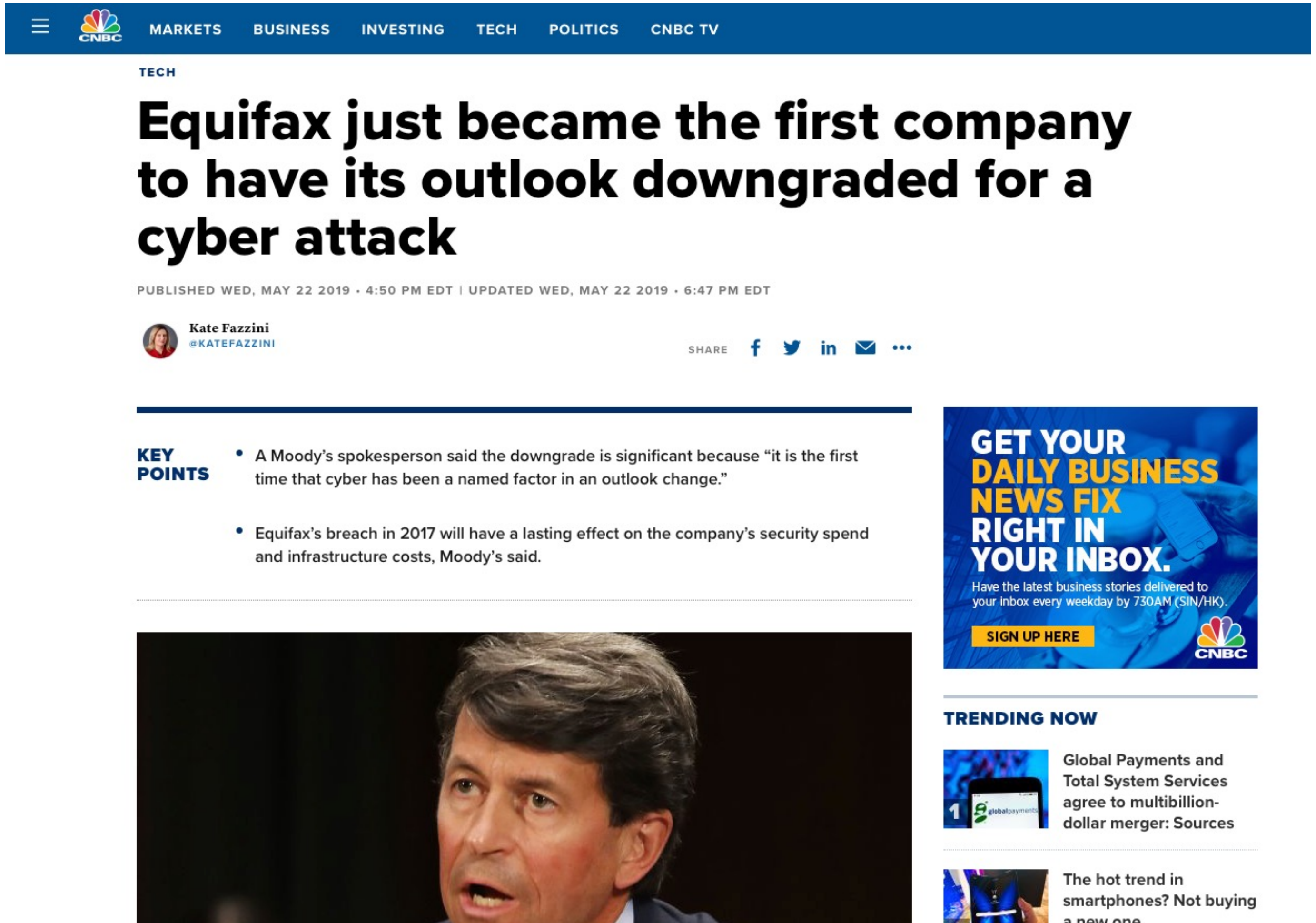
Malcolm Turnbull
@TurnbullMalcolm

We filled in the @ABSCensus tonight online - v easy to do. And so important for planning better Govt services & investment for the future

RETWEETS 205 LIKES 352

7:17 pm - 9 Aug 2016

Equifax Downgraded by Moody’s (cnbc.com)



TECH

Equifax just became the first company to have its outlook downgraded for a cyber attack

PUBLISHED WED, MAY 22 2019 • 4:50 PM EDT | UPDATED WED, MAY 22 2019 • 6:47 PM EDT

Kate Fazzini
@KATEFAZZINI

KEY POINTS

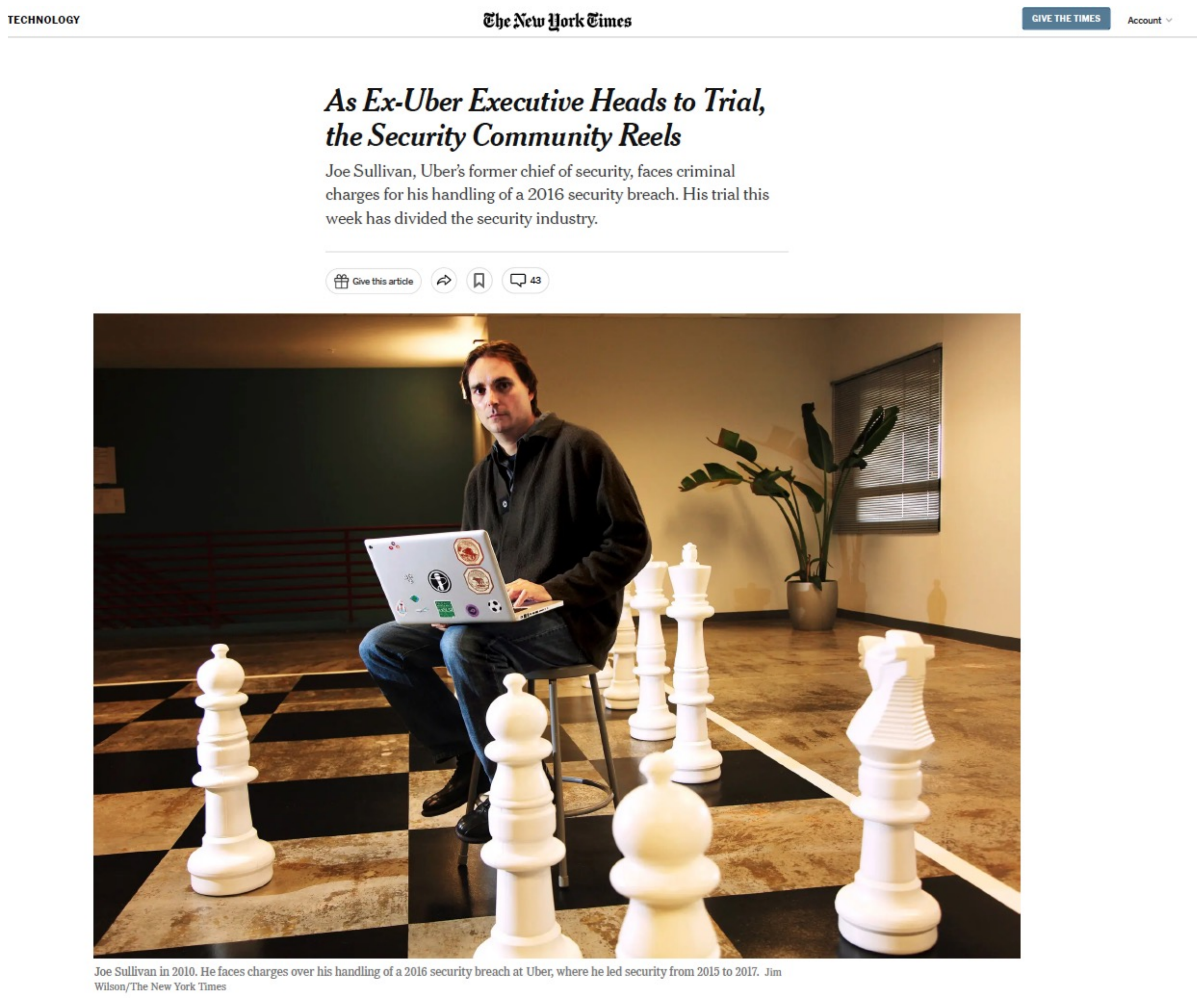
- A Moody’s spokesperson said the downgrade is significant because “it is the first time that cyber has been a named factor in an outlook change.”
- Equifax’s breach in 2017 will have a lasting effect on the company’s security spend and infrastructure costs, Moody’s said.

TRENDING NOW

1 Global Payments and Total System Services agree to multibillion-dollar merger: Sources

The hot trend in smartphones? Not buying a new one

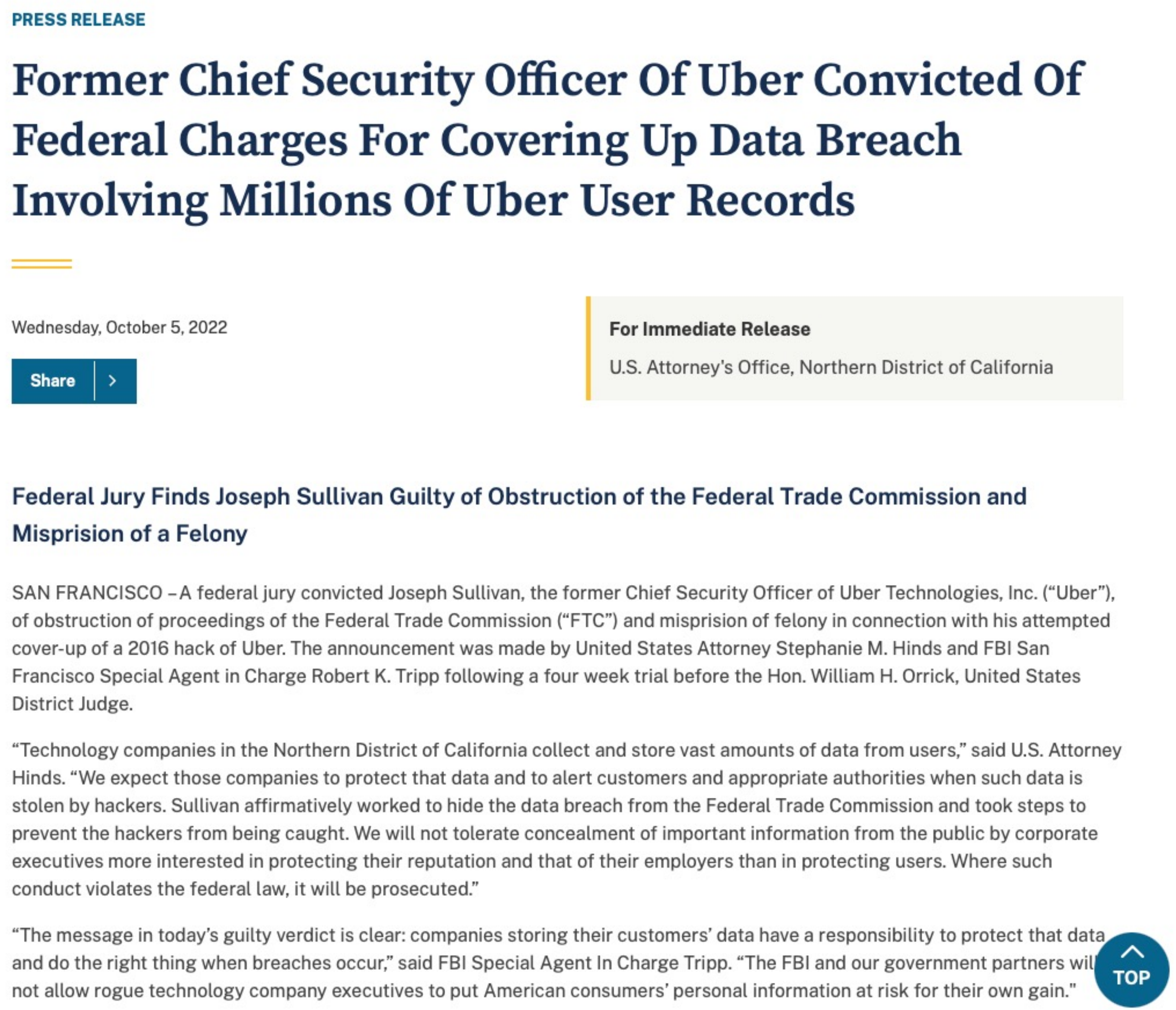
Uber CISO faces criminal trial



As Ex-Uber Executive Heads to Trial, the Security Community Reels

Joe Sullivan, Uber's former chief of security, faces criminal charges for his handling of a 2016 security breach. His trial this week has divided the security industry.

Joe Sullivan in 2010. He faces charges over his handling of a 2016 security breach at Uber, where he led security from 2015 to 2017. Jim Wilson/The New York Times



PRESS RELEASE

Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records

Wednesday, October 5, 2022

For Immediate Release

U.S. Attorney's Office, Northern District of California

Federal Jury Finds Joseph Sullivan Guilty of Obstruction of the Federal Trade Commission and Misprision of a Felony

SAN FRANCISCO – A federal jury convicted Joseph Sullivan, the former Chief Security Officer of Uber Technologies, Inc. (“Uber”), of obstruction of proceedings of the Federal Trade Commission (“FTC”) and misprision of felony in connection with his attempted cover-up of a 2016 hack of Uber. The announcement was made by United States Attorney Stephanie M. Hinds and FBI San Francisco Special Agent in Charge Robert K. Tripp following a four week trial before the Hon. William H. Orrick, United States District Judge.

“Technology companies in the Northern District of California collect and store vast amounts of data from users,” said U.S. Attorney Hinds. “We expect those companies to protect that data and to alert customers and appropriate authorities when such data is stolen by hackers. Sullivan affirmatively worked to hide the data breach from the Federal Trade Commission and took steps to prevent the hackers from being caught. We will not tolerate concealment of important information from the public by corporate executives more interested in protecting their reputation and that of their employers than in protecting users. Where such conduct violates the federal law, it will be prosecuted.”

“The message in today’s guilty verdict is clear: companies storing their customers’ data have a responsibility to protect that data and do the right thing when breaches occur,” said FBI Special Agent In Charge Tripp. “The FBI and our government partners will not allow rogue technology company executives to put American consumers’ personal information at risk for their own gain.”

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

Exercise Conduct

- You will work in your normal roles (some will change as we go along i.e., shift change, availability)
- Exercise injects will be provided as you go along
- You will work thru the scenario in your assigned role
- At the end we will have a media conference

Disclaimer

- This scenario is entirely fictitious.
- All names, characters, and incidents portrayed in this workshop are fictitious.
- No identification with actual persons (living or deceased), places, buildings, and products is intended or should be inferred.
- Any references to actual international entities or persons is purely for dramatic effect

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

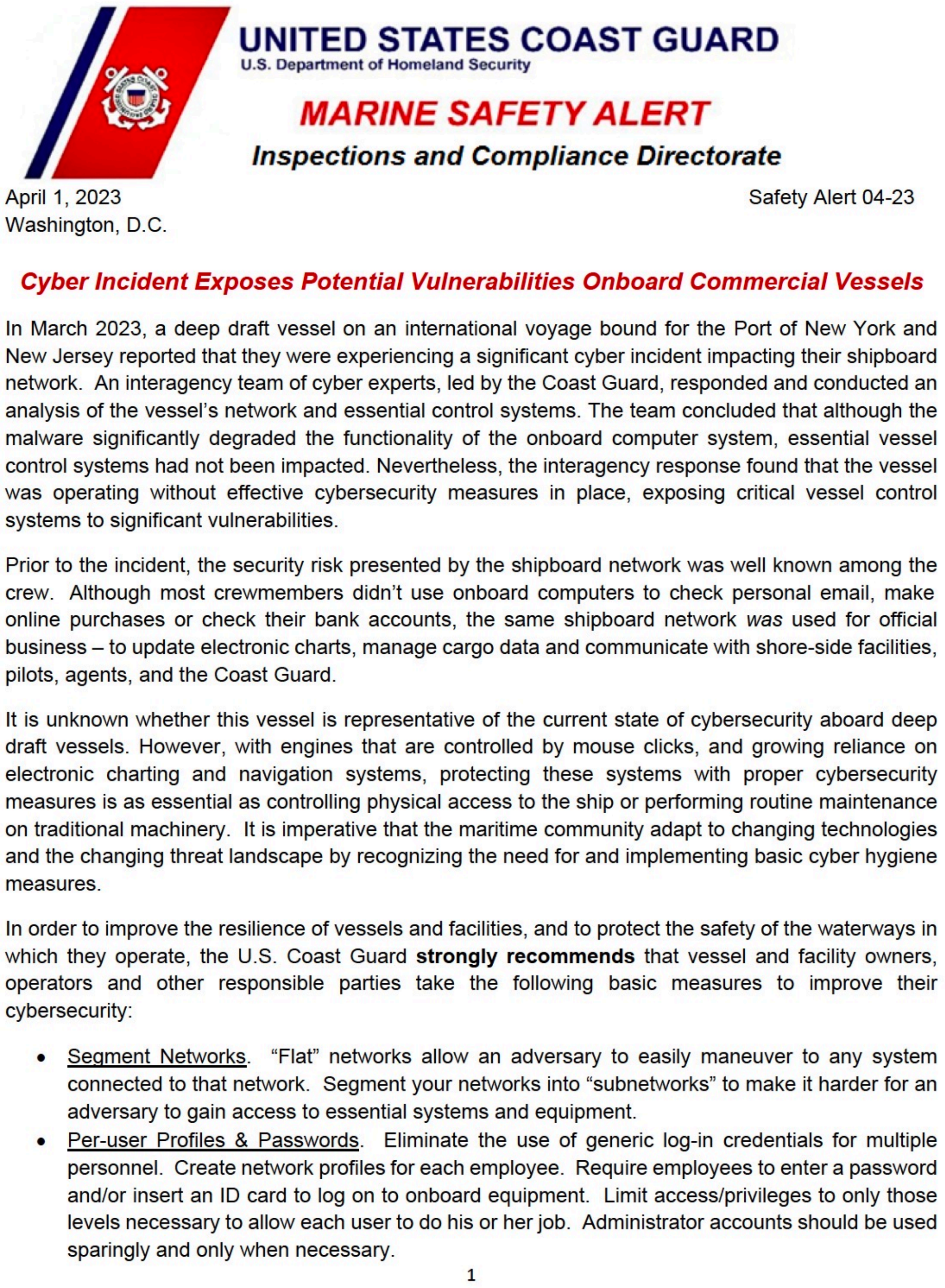
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

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.



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

MARINE SAFETY ALERT

Inspections and Compliance Directorate

April 1, 2023 Safety Alert 04-23
Washington, D.C.

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

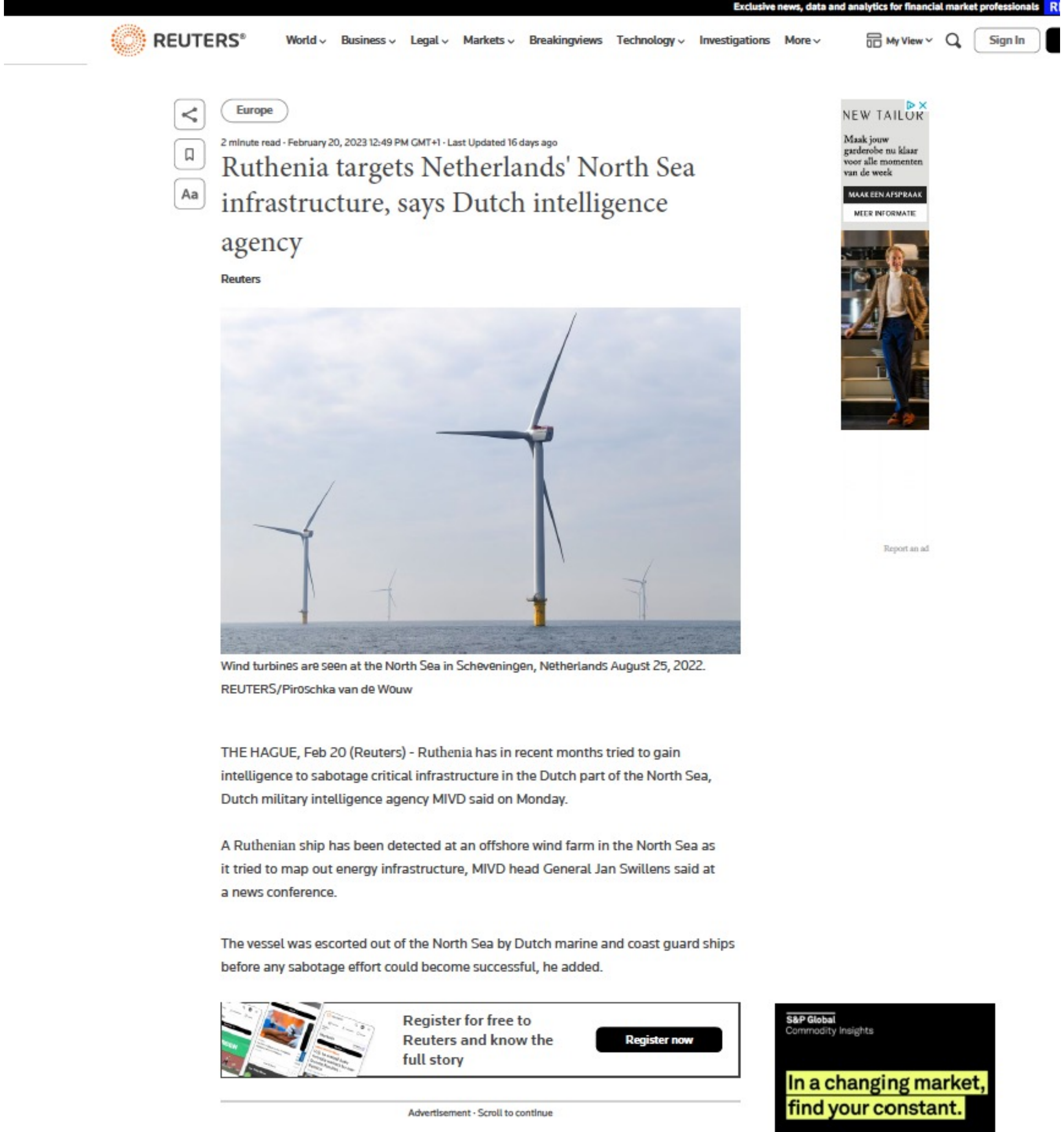
In March 2023, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis 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.

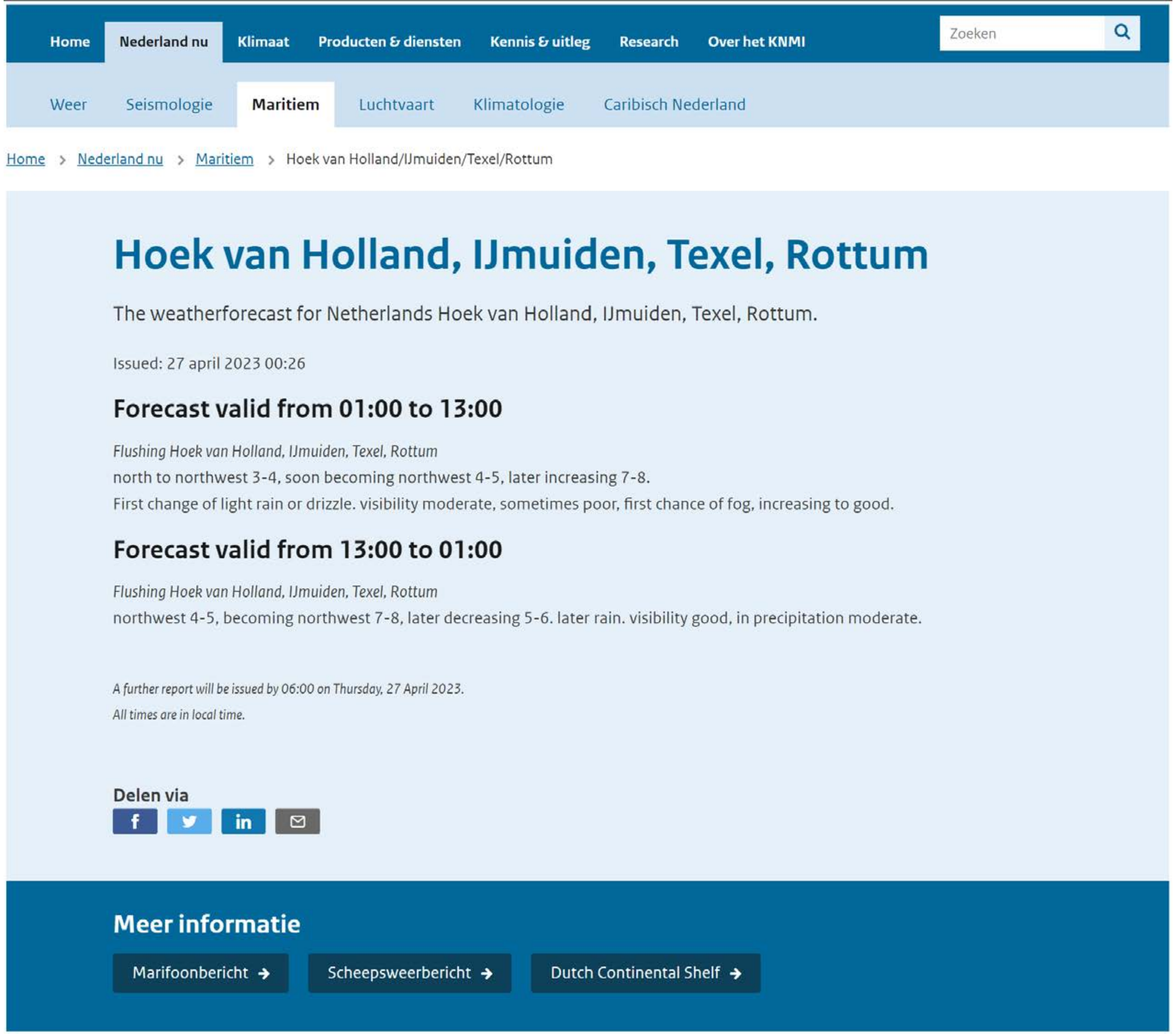
The vessel was escorted out of the North Sea by Dutch marine and coast guard ships before any sabotage effort could become successful, he added.

Lets begin

- Bring an Open Mind
- Accept the “Scenario Reality”
- Be ready to collaborate with others in your group
- Be ready to play the role you are assigned in front of the entire audience

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



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

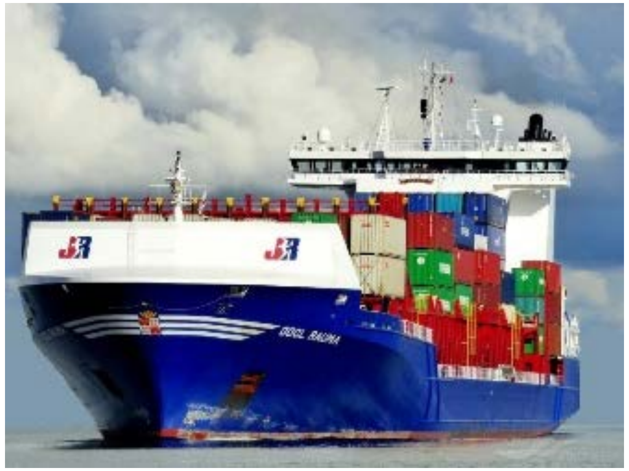
Flushing Hoek van Holland, IJmuiden, Texel, Rottum

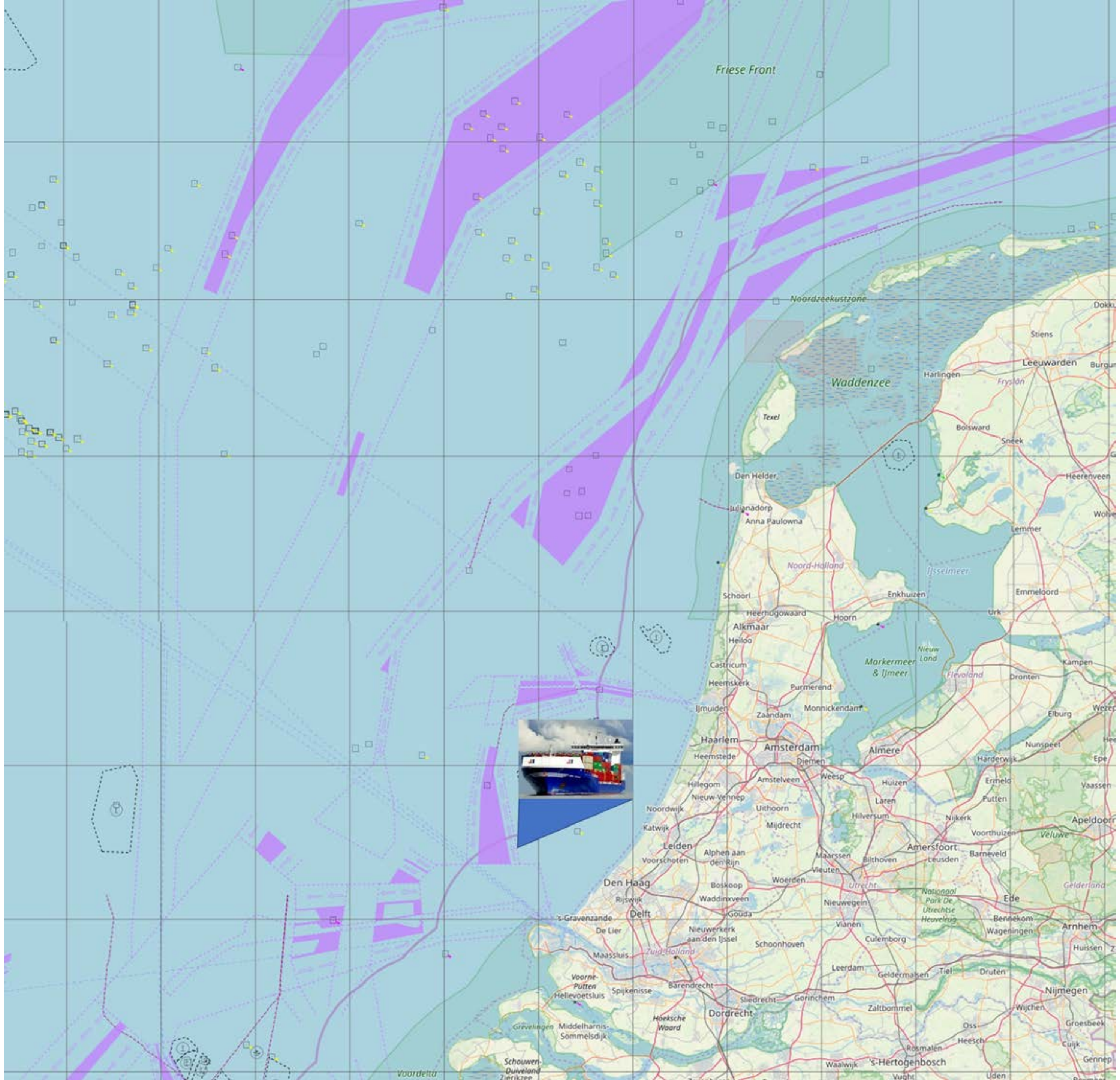
northwest 4-5, becoming northwest 7-8, later decreasing 5-6. later rain. visibility good, in precipitation moderate.

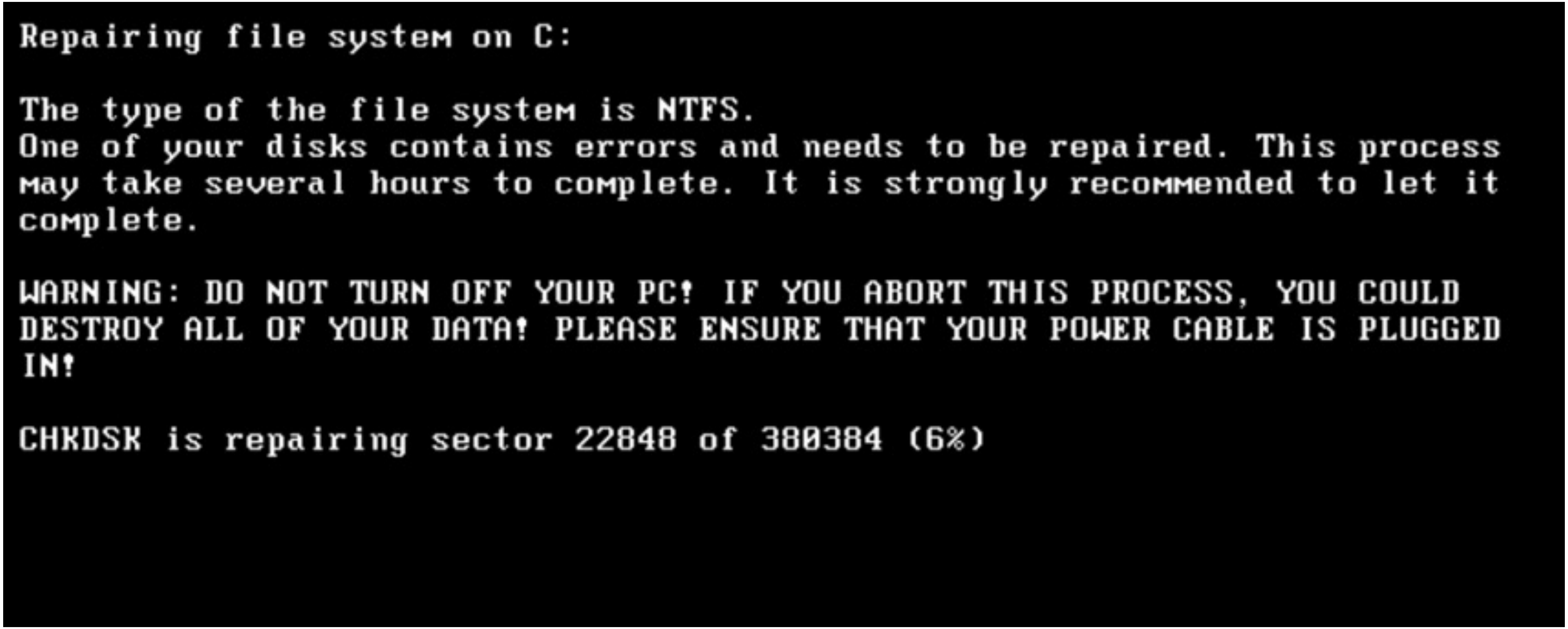
A further report will be issued by 06:00 on Thursday, 27 April 2023.

All times are in local time.

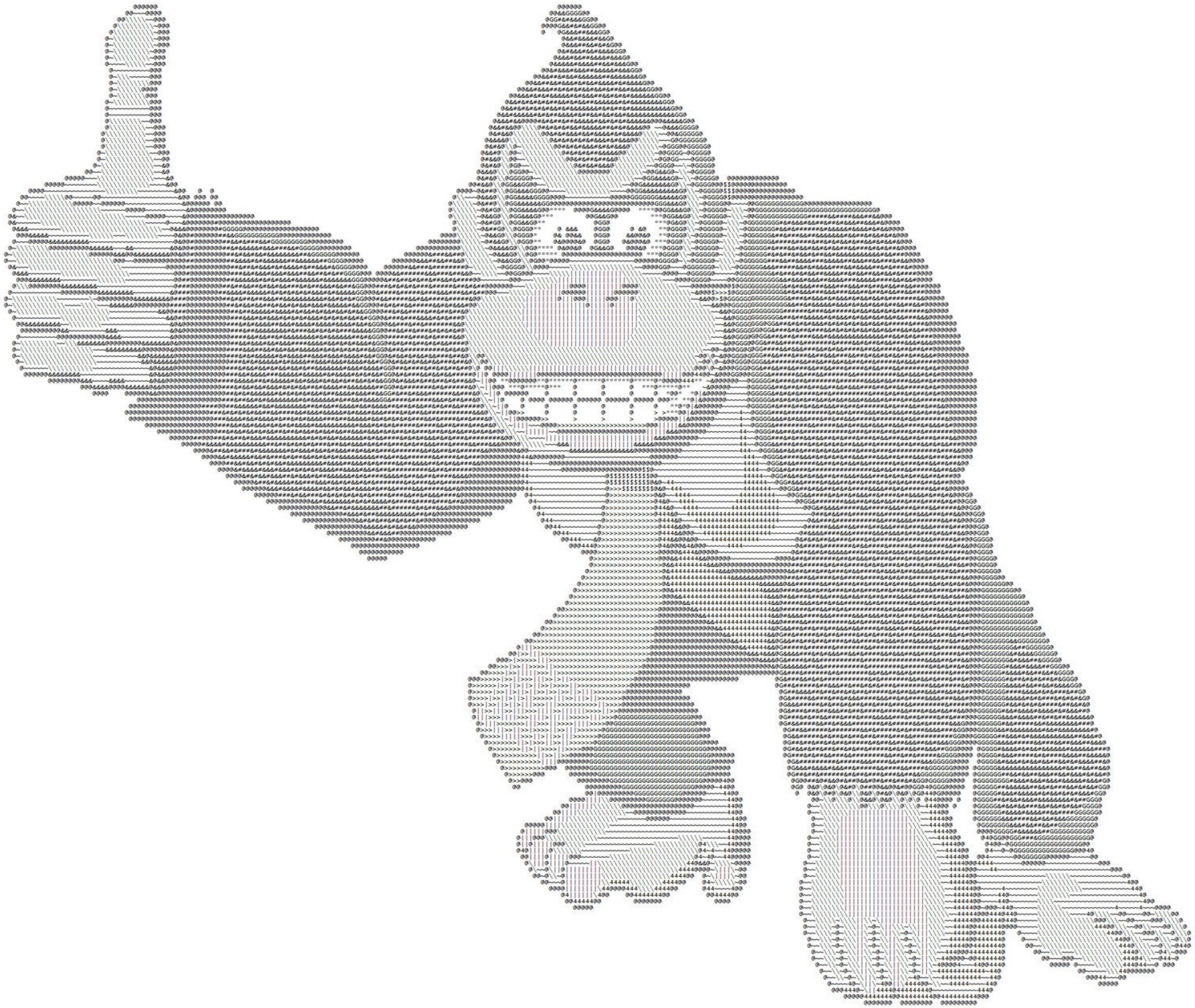
Position (GPS)
Lat: N:53°21.9712
Lon: E:005°13.3125
Time of position: 15:32
MMSI: 245401000
UTC: 2023/04/27 15:32

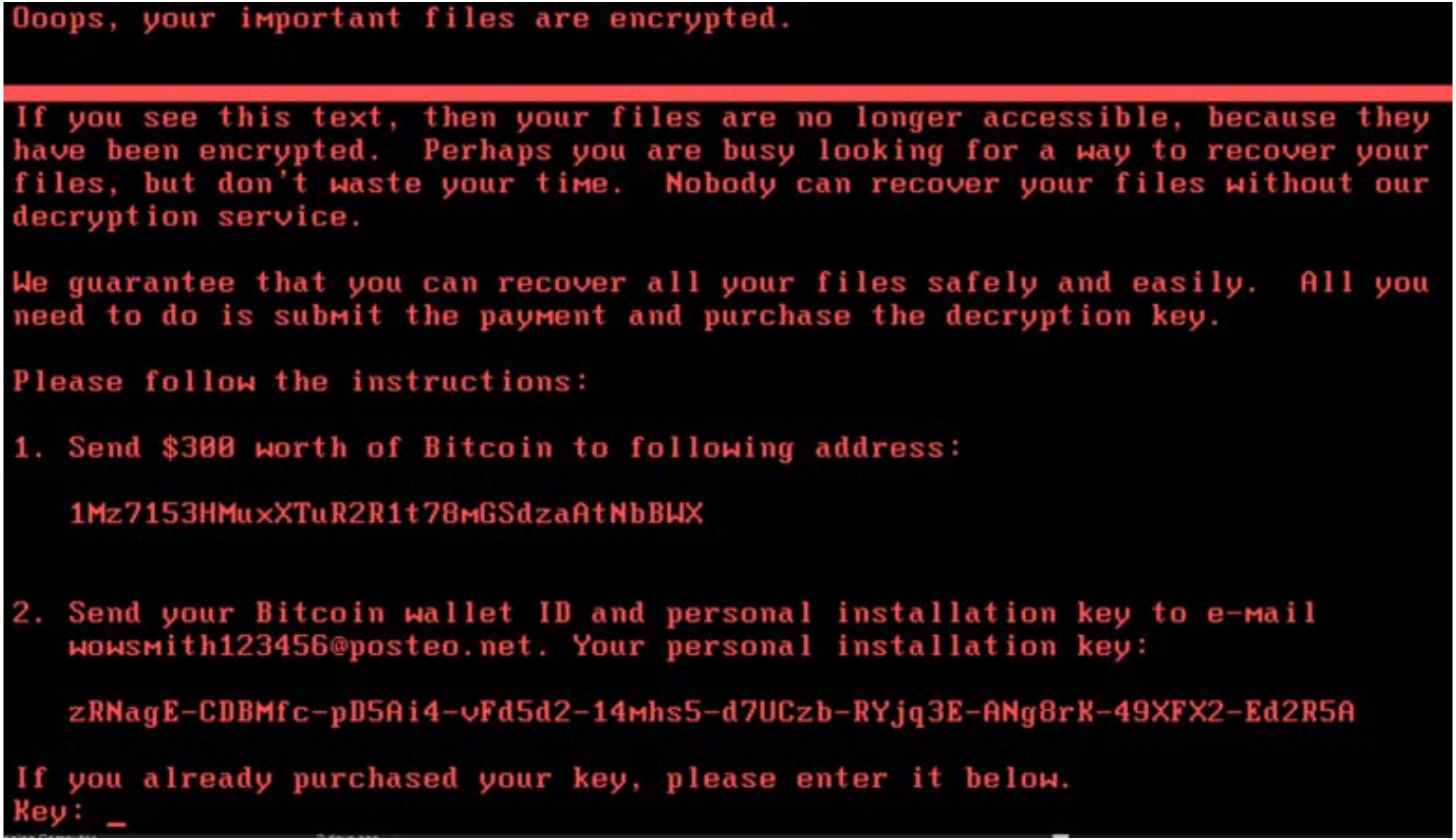
No.1	Name vessel:	**OOCL Rauma**
	Callsign:	PBWS
	Length/width:	169 m / 27 m
	Draft:	9,30 metre
	Persons on board:	15
	Destination:	Helsinki Via NOK
	Position:	52° 10, 32 North 003°54,4 East 1,5’ east Oil rigg P15E
	Course	351°
	Speed	drifting
	Cargo	General cargo in containers
	Dangerous cargo:	Yes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


Friese Front
Noordzeekustzone
Waddenzee
Texel
Den Helder
Julianadorp
Anna Paulowna
Harlingen
Leeuwarden
Fryslân
Stiens
Dokkum
Burgum
Bolsward
Sneek
Heerenveen
Wolvega
Lemmer
IJsselmeer
Noord-Holland
Schoorl
Enkhuizen
Emmeloord
Urk
Heerhugowaard
Hoorn
Alkmaar
Heiloo
Castricum
Heemskerk
Purmerend
Markermeer & IJmeer
Nieuw Land
Flevoland
Dronten
Kampen
IJmuiden
Monnickendam
Zaandam
Elburg
Haarlem
Amsterdam
Almere
Heemstede
Diemen
Nunspeet
Harderwijk
Hillegom
Amstelveen
Weesp
Huizen
Ermelo
Nieuw-Vennep
Laren
Putten
Noordwijk
Uithoorn
Hilversum
Nijkerk
Apeldoorn
Katwijk
Mijdrecht
Voorthuizen
Leiden
Alphen aan den Rijn
Maarssen
Amersfoort
Barneveld
Veluwe
Voorschoten
Bilthoven
Leusden
Vleuten
Utrecht
Den Haag
Boskoop
Woerden
Nationaal Park De Utrechtse Heuvelrug
Ede
Gelderland
Rijswijk
Waddinxveen
Nieuwegein
Delft
Gouda
Bennekom
's-Gravenzande
Vianen
Wageningen
Arnhem
De Lier
Nieuwerkerk aan den IJssel
Culemborg
Huissen
Maassluis
Zuid-Holland
Schoonhoven
Voorne-Putten
Leerdam
Geldermalsen
Tiel
Druten
Nijmegen
Hellevoetsluis
Spijkenisse
Barendrecht
Sliedrecht
Gorinchem
Wijchen
Zaltbommel
Groesbeek
Dordrecht
Hoeksche Waard
Grevelingen
Middelharnis-Sommelsdijk
Oss
Cuijk
Heesch
Rosmalen
Gennep
Schouwen-Duiveland
Zierikzee
Voordelta
Waalwijk
's-Hertogenbosch
Vught
Uden



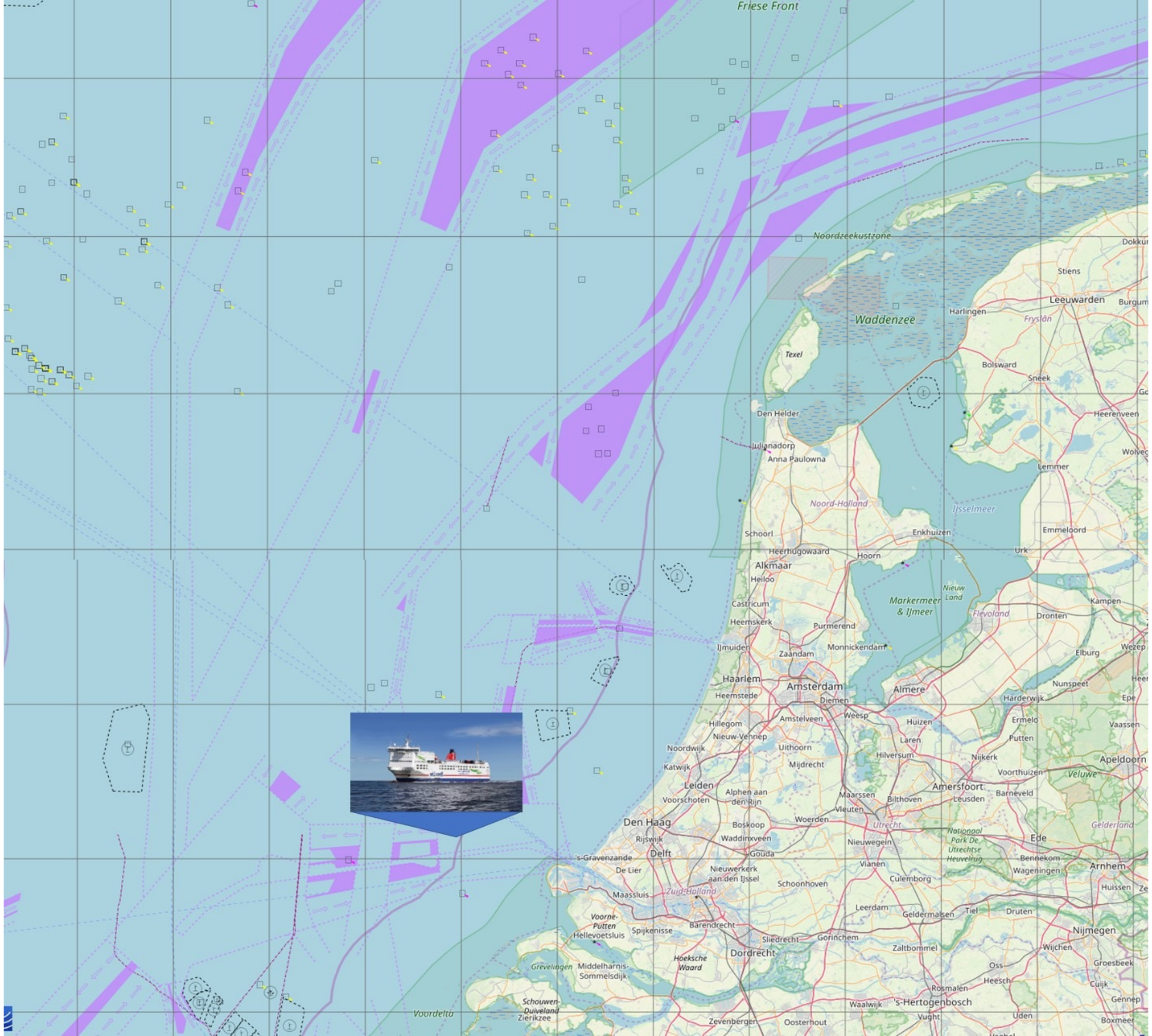
```
Repairing file system on C:

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%)
```





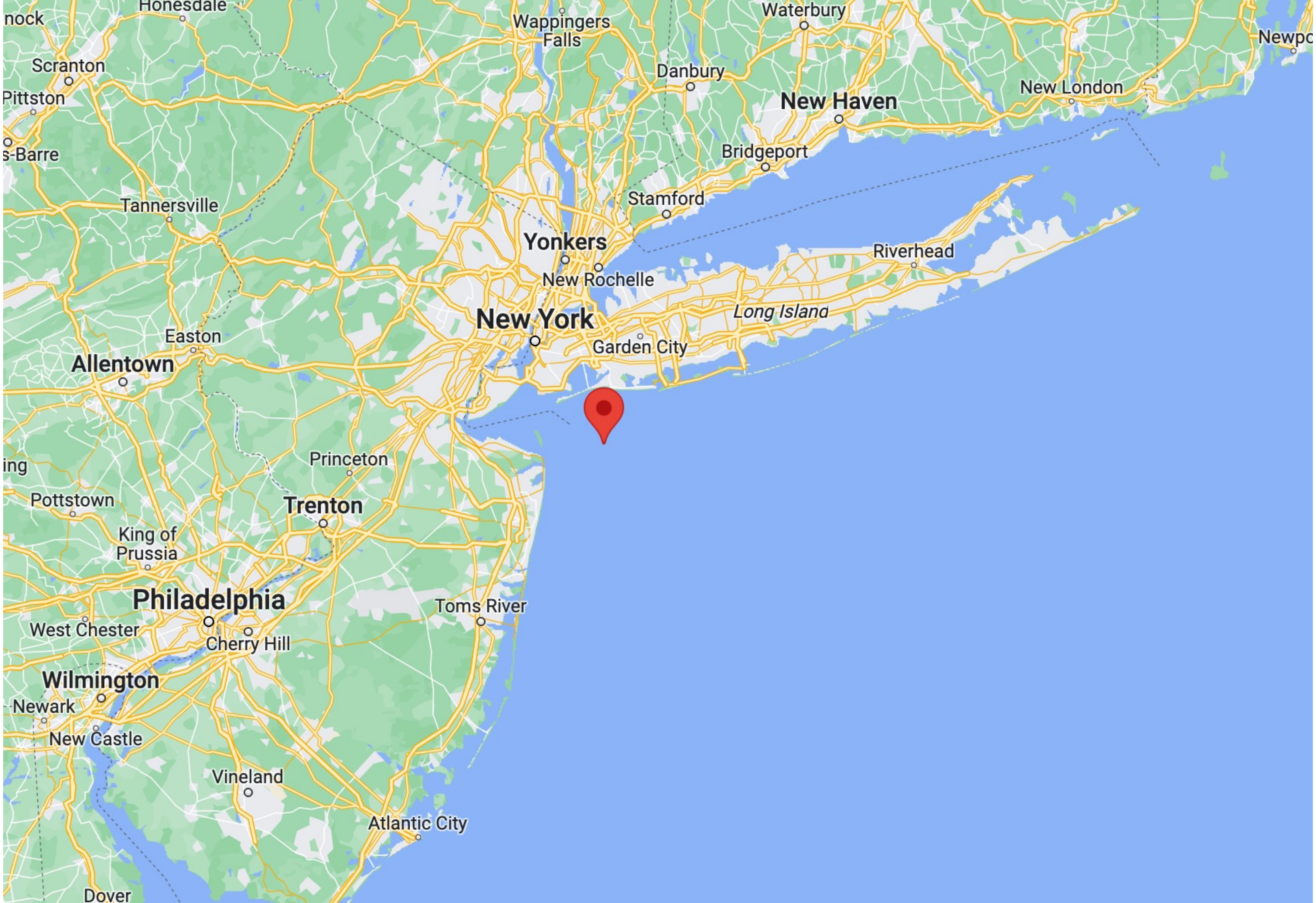
```
Ooops, your important files are encrypted.

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:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


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

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

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

No.2	Name vessel:	**Stena Transit**
	Callsign:	PHJU
	Length/width:	212 m / 31,6 m
	Draft:	5,8 m
	Persons on board:	100 crew and 300 passengers
	Destination:	Killingholme, GB
	Position:	North Maas Centre buoy 52° 10, 32 North 003°54,4 East
	Course	276°
	Speed	18 knots
	Cargo	Trailers /cars /passengers
	Dangerous cargo:	no
	Picture:	
	Owner:	P&O Ferries
	Flag:	Dutch
	IMO	9469388
	MMSI	244513000


Friese Front
Noordzeekustzone
Waddenzee
Texel
Den Helder
Julianadorp
Anna Paulowna
Noord-Holland
Schoorl
Heerhugowaard
Alkmaar
Heiloo
Castricum
Heemskerk
IJmuiden
Zaandam
Purmerend
Monnickendam
Hoorn
Enkhuizen
Markermeer & IJmeer
Nieuw Land
IJsselmeer
Haarlem
Heemstede
Amsterdam
Diemen
Almere
Weesp
Amstelveen
Hillegom
Nieuw-Vennep
Uithoorn
Mijdrecht
Noordwijk
Katwijk
Leiden
Voorschoten
Alphen aan den Rijn
Den Haag
Rijswijk
Delft
's-Gravenzande
De Lier
Maassluis
Zuid-Holland
Boskoop
Waddinxveen
Gouda
Nieuwerkerk aan den IJssel
Schoonhoven
Woerden
Maarssen
Vleuten
Utrecht
Nieuwegein
Vianen
Culemborg
Leerdam
Gorinchem
Sliedrecht
Zaltbommel
Geldermalsen
Tiel
Druten
Voorne-Putten
Hellevoetsluis
Spijkenisse
Barendrecht
Dordrecht
Hoeksche Waard
Grevelingen
Middelharnis-Sommelsdijk
Schouwen-Duiveland
Zierikzee
Voordelta
Zevenbergen
Oosterhout
Waalwijk
's-Hertogenbosch
Vught
Rosmalen
Oss
Heesch
Uden
Huizen
Laren
Hilversum
Bilthoven
Amersfoort
Leusden
Nationaal Park De Utrechtse Heuvelrug
Ede
Bennekom
Wageningen
Arnhem
Huissen
Nijmegen
Wijchen
Groesbeek
Cuijk
Gennep
Boxmeer
Gelderland
Barneveld
Voorthuizen
Nijkerk
Putten
Ermelo
Harderwijk
Nunspeet
Epe
Vaassen
Apeldoorn
Veluwe
Elburg
Dronten
Kampen
Flevoland
Emmeloord
Urk
Lemmer
Wolvega
Heerenveen
Sneek
Bolsward
Harlingen
Fryslân
Leeuwarden
Stiens
Dokkum
Burgum

UNITED STATES COAST GUARD

CYBER COMMAND


nock
Honesdale
Wappingers Falls
Waterbury
Newpo
Scranton
Pittston
Danbury
New Haven
New London
s-Barre
Bridgeport
Stamford
Tannersville
Yonkers
Riverhead
New Rochelle
New York
Long Island
Easton
Allentown
Garden City
Princeton
ing
Pottstown
Trenton
King of Prussia
Philadelphia
Toms River
West Chester
Cherry Hill
Wilmington
Newark
New Castle
Vineland
Atlantic City
Dover

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:	
	Owner:	DAIICHI CHUO MARINE - TOKYO, JAPAN
	Flag	Hong Kong
	IMO number	9515187
	MMSI	477045300

Free Play – Group Discussion

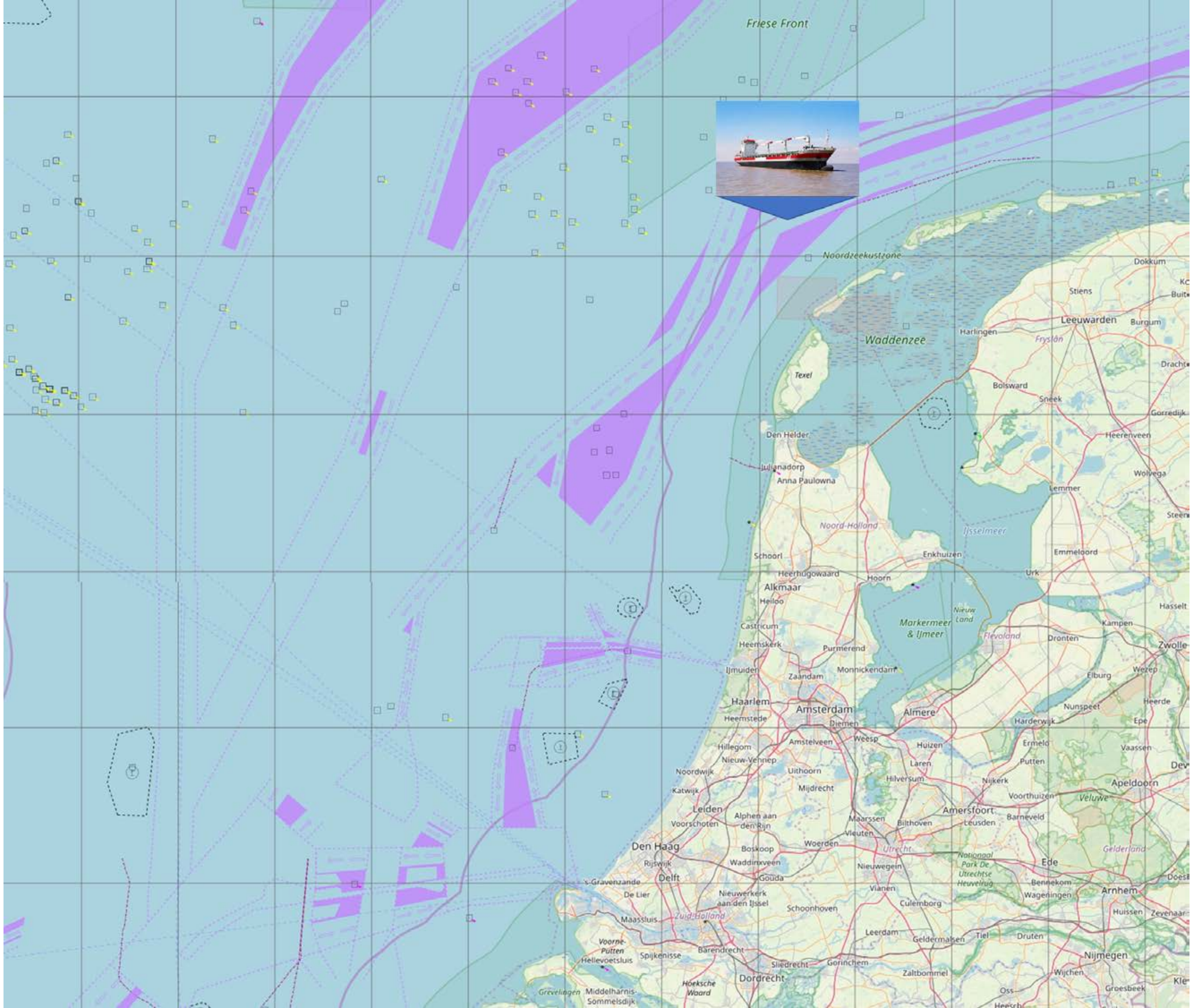
- What is going on?
- Response activities
- Who do you inform
- Do we need to take further action?
- Next steps?

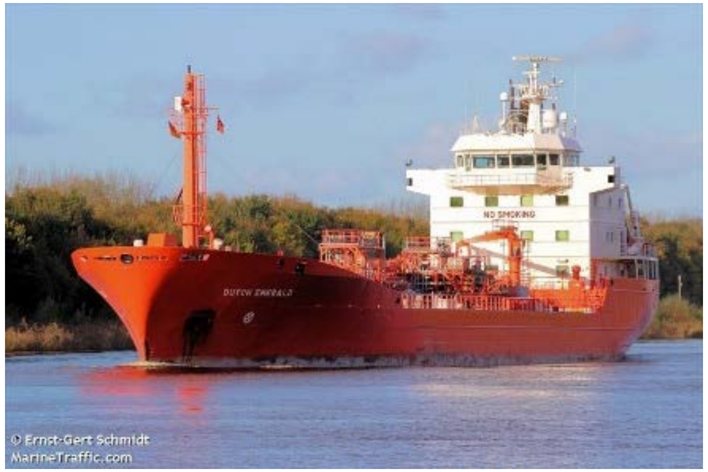
Dilemma Session Agenda

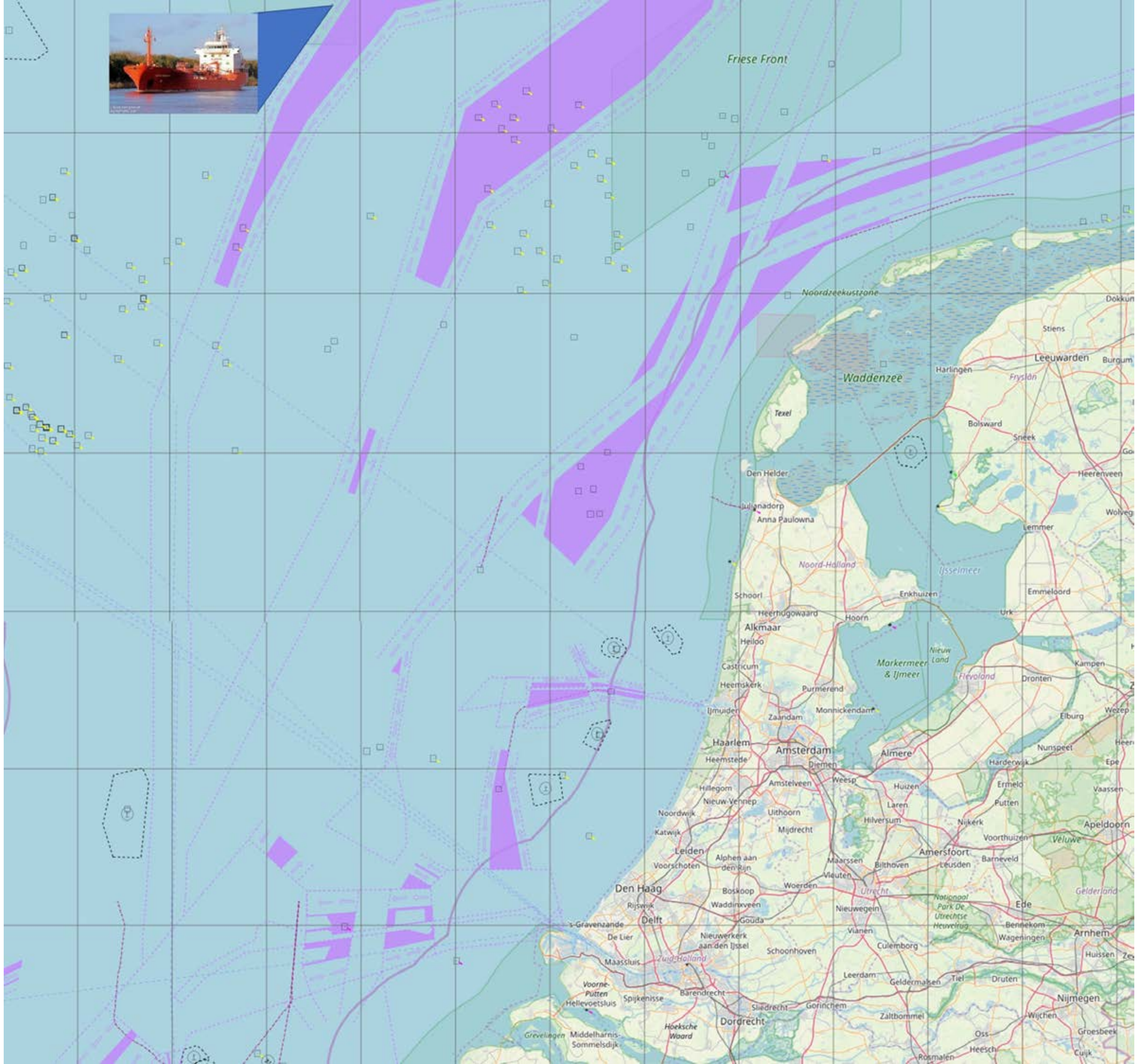
1300 – 1345	• Introduction
1345 – 1400	• Incident Conduct & Scenario Intro
1400 – 1430	• Part 1 0600 HRS
1430 – 1500	• Part 2 1200 HRS
1500 – 1530	• Part 3 1800 HRS
1530 – 1545	• Press conference role play
1545 – 1630	• Exercise Wash-up/Wrap up

NEWS
MEDIA CHANNEL
PRESS
MEDIA CHANNEL
TV
NEWS NETWORK
NEWS CHANNEL
NEWS CHANNEL
TV CHANNEL
NEWS CHANNEL
MEDIA
TV NETWORK
PRESS
TV
RADIO
TV
MEDIA
MEDIA
TV NETWORK
PRESS
TV
PRESS
NEWS

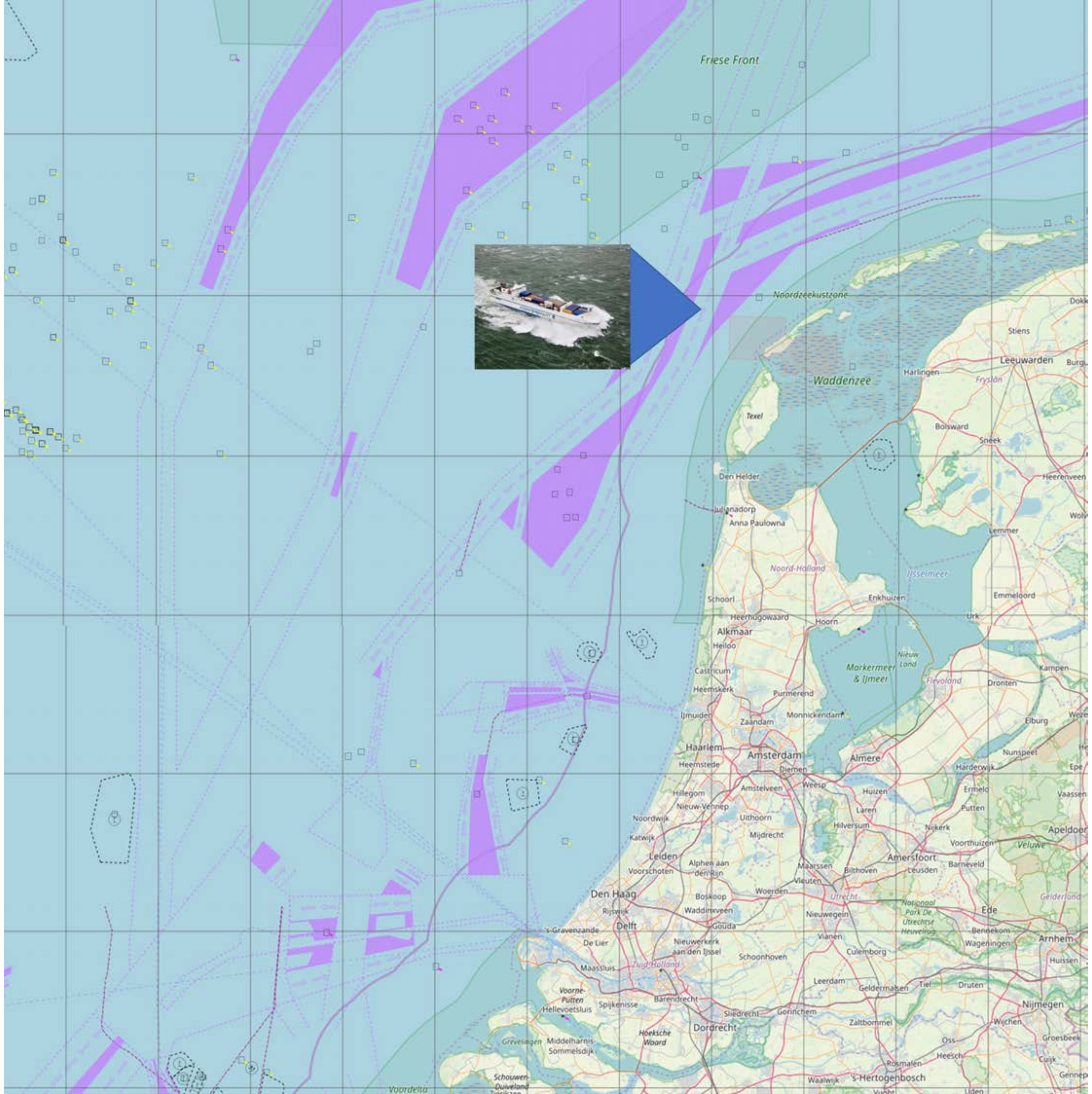
No.4	Name vessel:	**Avonborg**
	Callsign:	PCOF
	Length/width:	142,92 m /21,54 m
	Draft:	5,5 m
	Persons on board:	17
	Destination:	Kotka (Finland) via NOK
	Position:	Passed VL 5 53° 24, 22 North 004°44,35 East
	Course	065°
	Speed	10 knots
	Cargo	Ballast
	Dangerous cargo:	no
	Picture:	
	Owner:	Wagenborg
	Flag	Dutch
	IMO number	9466362
	MMSI	246865000


Friese Front
Noordzeekustzone
Waddenzee
Texel
Den Helder
Julianadorp
Anna Paulowna
Noord-Holland
Schoorl
Heerhugowaard
Alkmaar
Heiloo
Castricum
Heemskerk
IJmuiden
Haarlem
Heemstede
Zaandam
Amsterdam
Diemen
Purmerend
Monnickendam
Markermeer & IJmeer
Hoorn
Enkhuizen
IJsselmeer
Nieuw Land
Flevoland
Almere
Hillegom
Nieuw-Vennep
Amstelveen
Uithoorn
Weesp
Huizen
Laren
Hilversum
Mijdrecht
Noordwijk
Katwijk
Leiden
Alphen aan den Rijn
Voorschoten
Den Haag
Rijswijk
Delft
's-Gravenzande
De Lier
Maassluis
Zuid-Holland
Voorne-Putten
Hellevoetsluis
Spijkenisse
Barendrecht
Sliedrecht
Dordrecht
Hoeksche Waard
Grevelingen
Middelharnis-Sommelsdijk
Boskoop
Waddinxveen
Gouda
Nieuwerkerk aan den IJssel
Schoonhoven
Woerden
Maarssen
Vleuten
Utrecht
Bilthoven
Nieuwegein
Vianen
Culemborg
Leerdam
Gorinchem
Zaltbommel
Geldermalsen
Tiel
Druten
Amersfoort
Leusden
Nationaal Park De Utrechtse Heuvelrug
Nijkerk
Barneveld
Ede
Bennekom
Wageningen
Arnhem
Huissen
Zevenaar
Nijmegen
Wijchen
Groesbeek
Oss
Doesb
Kle
Gelderland
Veluwe
Apeldoorn
Voorthuizen
Putten
Ermelo
Harderwijk
Vaassen
Epe
Heerde
Dev
Nunspeet
Elburg
Wezep
Zwolle
Kampen
Dronten
Hasselt
Urk
Emmeloord
Lemmer
Steen
Wolvega
Heerenveen
Gorredijk
Sneek
Bolsward
Drachten
Harlingen
Fryslân
Leeuwarden
Burgum
Stiens
Dokkum
Buit
Kc

No.5	Name vessel:	**Dutch Emerald**
	Callsign:	PCIP
	Length/width:	118 m /17,03
	Draft:	5,4 m
	Persons on board:	10
	Destination:	Antwerpen
	Position:	East of K1A 53° 50, 49 North 003°09,33 East
	Course	212°
	Speed	9 knots
	Cargo	5000 T Benzeen
	Dangerous cargo:	yes
	Picture:	
	Owner:	Essenberger -Hamburg Germany
	Flag	Dutch
	IMO number	9191668
	MMSI	246436000


Friese Front
Noordzeekustzone
Waddenzee
Texel
Dokkum
Stiens
Leeuwarden
Burgum
Harlingen
Fryslân
Bolsward
Sneek
Heerenveen
Wolvega
Lemmer
Den Helder
Julianadorp
Anna Paulowna
Noord-Holland
IJsselmeer
Schoorl
Emmeloord
Enkhuizen
Urk
Heerhugowaard
Hoorn
Alkmaar
Heiloo
Castricum
Heemskerk
Purmerend
Markermeer & IJmeer
Nieuw Land
Flevoland
Dronten
Kampen
IJmuiden
Zaandam
Monnickendam
Elburg
Wezep
Haarlem
Amsterdam
Almere
Nunspeet
Heemstede
Diemen
Harderwijk
Epe
Amstelveen
Weesp
Ermelo
Vaassen
Hillegom
Nieuw-Vennep
Huizen
Putten
Noordwijk
Uithoorn
Laren
Hilversum
Katwijk
Mijdrecht
Nijkerk
Voorthuizen
Veluwe
Apeldoorn
Leiden
Alphen aan den Rijn
Amersfoort
Barneveld
Voorschoten
Maarssen
Bilthoven
Leusden
Den Haag
Boskoop
Woerden
Utrecht
Vleuten
Nationaal Park De Utrechtse Heuvelrug
Ede
Gelderland
Rijswijk
Waddinxveen
Delft
Gouda
Nieuwegein
Bennekom
's-Gravenzande
Wageningen
Arnhem
De Lier
Nieuwerkerk aan den IJssel
Vianen
Maassluis
Zuid-Holland
Schoonhoven
Culemborg
Huissen
Voorne-Putten
Spijkenisse
Leerdam
Geldermalsen
Tiel
Druten
Hellevoetsluis
Barendrecht
Sliedrecht
Gorinchem
Nijmegen
Zaltbommel
Wijchen
Hoeksche Waard
Dordrecht
Grevelingen
Middelharnis-Sommelsdijk
Oss
Groesbeek
Heesch
Cuijk
Rosmalen

No.6	Name vessel:	**Kraftka**
	Callsign:	PHGY
	Length/width:	205 m /25,8 m
	Draft:	8,1 m
	Persons on board:	20
	Destination:	Gdynia Poland via Eemshaven Netherlands
	Position:	Just passed the VL 3 53° 18, 68 North 004°38,9 East
	Course	022°
	Speed	12 knots
	Cargo	Military goods (US) Trucks, tanks etc
	Dangerous cargo:	Yes Ammunition
	Picture:	
	Owner:	Spliethof
	Flag	Dutch
	IMO number	9307360
	MMSI	246554000


Friese Front
Noordzeekustzone
Waddenzee
Texel
Den Helder
Julianadorp
Anna Paulowna
Noord-Holland
Schoorl
Heerhugowaard
Alkmaar
Heiloo
Castricum
Heemskerk
IJmuiden
Zaandam
Haarlem
Heemstede
Amsterdam
Diemen
Hillegom
Nieuw-Vennep
Noordwijk
Katwijk
Leiden
Voorschoten
Den Haag
Rijswijk
Delft
's-Gravenzande
De Lier
Maassluis
Zuid-Holland
Voorne-Putten
Hellevoetsluis
Spijkenisse
Barendrecht
Dordrecht
Hoeksche Waard
Grevelingen
Middelharnis-Sommelsdijk
Schouwen-Duiveland
Voordelta
Stiens
Leeuwarden
Harlingen
Fryslân
Bolsward
Sneek
Heerenveen
Lemmer
IJsselmeer
Enkhuizen
Hoorn
Emmeloord
Urk
Markermeer & IJmeer
Nieuw Land
Flevoland
Dronten
Kampen
Purmerend
Monnickendam
Almere
Elburg
Nunspeet
Harderwijk
Ermelo
Putten
Huizen
Laren
Hilversum
Weesp
Amstelveen
Uithoorn
Mijdrecht
Alphen aan den Rijn
Boskoop
Waddinxveen
Gouda
Woerden
Maarssen
Utrecht
Bilthoven
Amersfoort
Leusden
Barneveld
Nijkerk
Voorthuizen
Veluwe
Apeldoorn
Vaassen
Epe
Ede
Bennekom
Wageningen
Arnhem
Huissen
Gelderland
Nationaal Park De Utrechtse Heuvelrug
Vianen
Nieuwegein
Culemborg
Schoonhoven
Nieuwerkerk aan den IJssel
Sliedrecht
Gorinchem
Leerdam
Geldermalsen
Tiel
Druten
Nijmegen
Wijchen
Groesbeek
Cuijk
Zaltbommel
Rosmalen
's-Hertogenbosch
Heesch
Oss
Waalwijk
Uden

KINGKONG TECHNICAL ANALYSIS

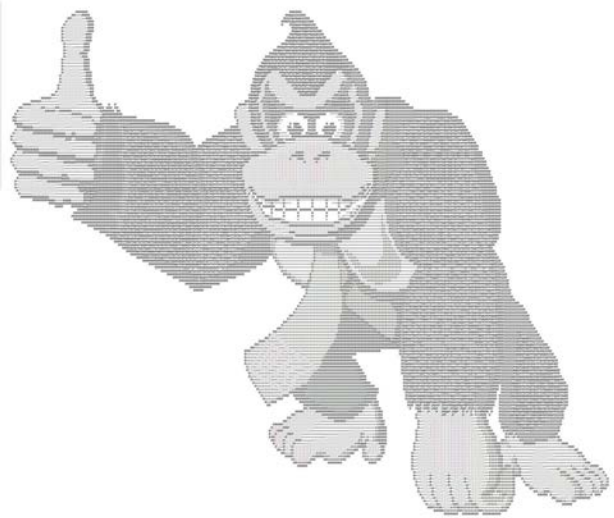
LogRhythm Labs

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.

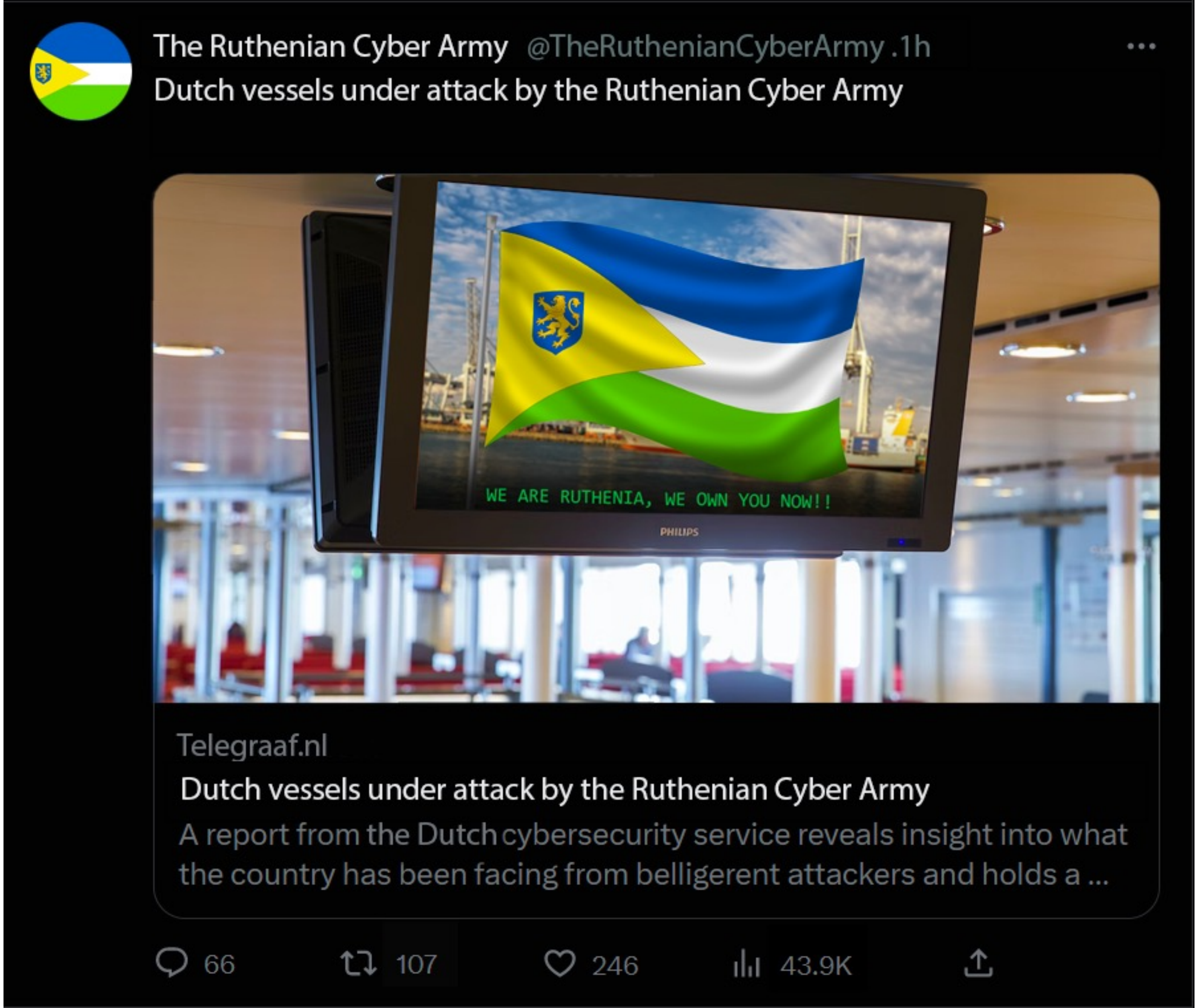
Free Play – Group Discussion

- What is going on?
- Response activities
- Who do you inform
- Do we need to take further action?
- Next steps?

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

NCL
诺唯真喜悦号 NORWEGIAN JOY



The Ruthenian Cyber Army @TheRuthenianCyberArmy .1h

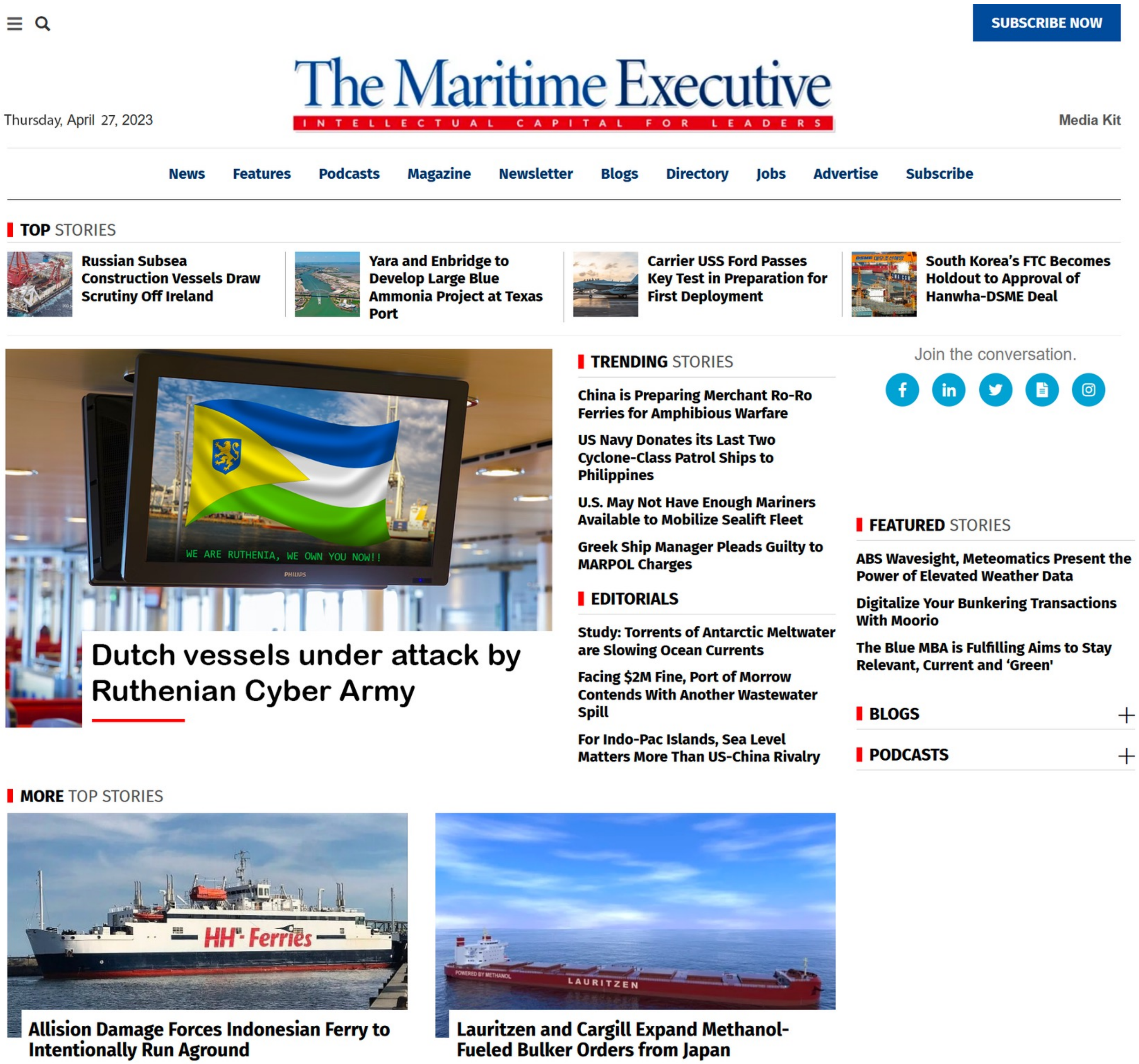
Dutch vessels under attack by the Ruthenian Cyber Army

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



SUBSCRIBE NOW

The Maritime Executive

INTELLECTUAL CAPITAL FOR LEADERS

Thursday, April 27, 2023

Media Kit

News · Features · Podcasts · Magazine · Newsletter · Blogs · Directory · Jobs · Advertise · Subscribe

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

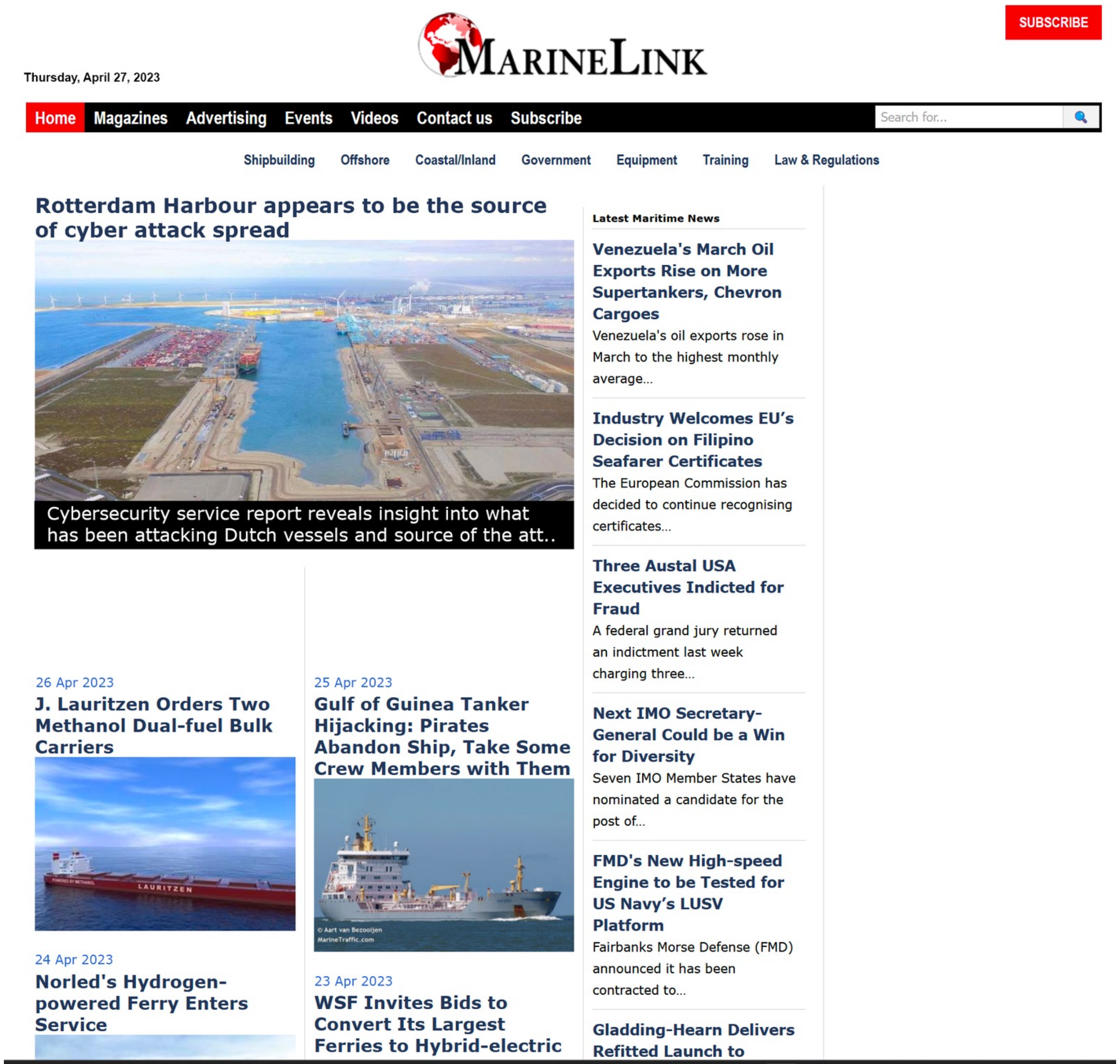
- ABS Wavesight, Meteomatics Present the Power of Elevated Weather Data
- Digitalize Your Bunkering Transactions With Moorio
- The Blue MBA is Fulfilling Aims to Stay Relevant, Current and 'Green'

BLOGS +

PODCASTS +

MORE TOP STORIES

- Allision Damage Forces Indonesian Ferry to Intentionally Run Aground
- Lauritzen and Cargill Expand Methanol-Fueled Bulker Orders from Japan



SUBSCRIBE

MARINELINK

Thursday, April 27, 2023

Home Magazines Advertising Events Videos Contact us Subscribe

Search for...

Shipbuilding Offshore Coastal/Inland Government Equipment Training Law & Regulations

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

25 Apr 2023

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

24 Apr 2023

Norled's Hydrogen-powered Ferry Enters Service

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.

NL Police Forensic Report

- The Shipmanagers software from Limany Group delivered the wiper-malware to the vessel through their API (Application program Interface) services.
- Limany Supply Group was compromised 1 month before by a Ruthenian state actor.
- When a vessel connects to Shipmangers servers through API calls the KingKong wiper-malware is delivered to the target.
- The destructive KingKong wiper-malware remained dormant until Kings Day 2023 when it was activated on the infected vessels.

POLITIE

Free Play – Group Discussion

- What is going on?
- Response activities
- Who do you inform
- Do we need to take further action?
- Next steps?

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

What now?

- This incident already involves six vessels and a nation state attacker Ruthenia
- How would you handle this situation?
- Who would you work with?
- What are some of crticial things you need to consider?
- What information do you need to try and resolve the incident?

Realistic?

- Malware was modelled on notPetya (2017)
- notPetya attack occurred on Ukrainian national holiday, Constitution Day
- Malware came from supply chain M.E.Doc updates server
- Similar impacts seen on bridge systems by malware
- Vulnerability of AutoPilot to false commands documented by University of Plymouth research
- Similar cyber attacks on infrastructure by Russia and others
- US Intelligence report real but about Russia

Thank you for your attention

NHL STENDEN

university of applied sciences