MARITIME CYBER SECURITY-AN OVERVIEW

COMMODORE UDAI RAO(RETD)
FORMER PRINCIPAL DIRECTOR NAVAL INTELLIGENCE
FORMER DIRECTOR CABINET SECRETARIAT

MARITIME CYBER SECURITY

- DISCLAIMER : NOT A CYBER SECURITY EXPERT
- EXPERIENCE IN MARITIME DOMAIN
- VULNERABILITIES , THREATS , IMPLICATIONS etc

MARITIME CYBER SECURITY

Maritime cyber risk refers to a measure of the **extent to which a technology asset could be threatened by a potential** circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

MARITIME CYBER SECURITY IS A ‘NICHE WITHIN A NICHE ‘ DISCIPLINE

- 90% OF WORLD'S CARGO GOES BY SEA
- 50, 000 SHIPS IN HARBOUR AND SEA ,AT ANY TIME –ESTIMATED
- INCREASING NUMBER OF PORTS & SHIPS WORLD WIDE

MARITIME ACTIVITY IS INVISIBLE – OUT OF SIGHT

TRANSPORTATION IS FAR FROM LAND – FAR FLUNG

FOREIGN LANDS

Global Maritime Traffic

SHIPPING LOGISTICS - MULTIPLE STAKE HOLDERS -WORLD WIDE

- SHIPPING COMPANIES
- SHIP OWNERS
- CUSTOM HOUSES
- STEVEDORES
- FREIGHT FORWARDERS
- SHIP CHANDLERS
- MARINE INSURANCE
- PORT AUTHORITIES
- SHIP MANAGEMENT COMPANIES
- WARE HOUSES

SHIPPING LOGISTICS - MULTIPLE STAKE HOLDERS -WORLD WIDE

- CONTAINER STUFFING & DE STUFFING STATIONS
- MARITIME BOARDS
- FLAG STATE
- PORT OF REGISTRATION
- CHARTERER
- CONSIGNOR
- CONSIGNEE
- TRANS-SHIPMENT PORT , eg COLOMBO

- SHIPPING ECO-SYSTEM - SYSTEM OF SYSTEMS

- LACK OF ACCOUNTABILITY

SHIPPING STAKEHOLDERS

- MOTIVE – PROFIT
- SAVE TIME
- SAVE FUEL
- SAVE MONEY
- SHORTEST NAVIGABLE ROUTES
- REDUCE OPERATING COSTS
- REDUCE MANNING COSTS
- PRESSURE TO LOAD & UNLOAD CARGO AND PUT TO SEA
- PROPELLOR TIME IS WHEN SHIP EARNS MONEY

- MARINERS –WEAK LINK – WORK MORE 18 H PER DAY
- MARITIME CYBER SECURITY AWARENESS IS JUST CATCHING ON IN SHIPPING CIRCLES .
- IMO RESOLUTION -2017

MULTI-MODAL TRANSPORTATION

INCREASES VULNERABILITY


NATIONAL PERMIT
CAPITAL

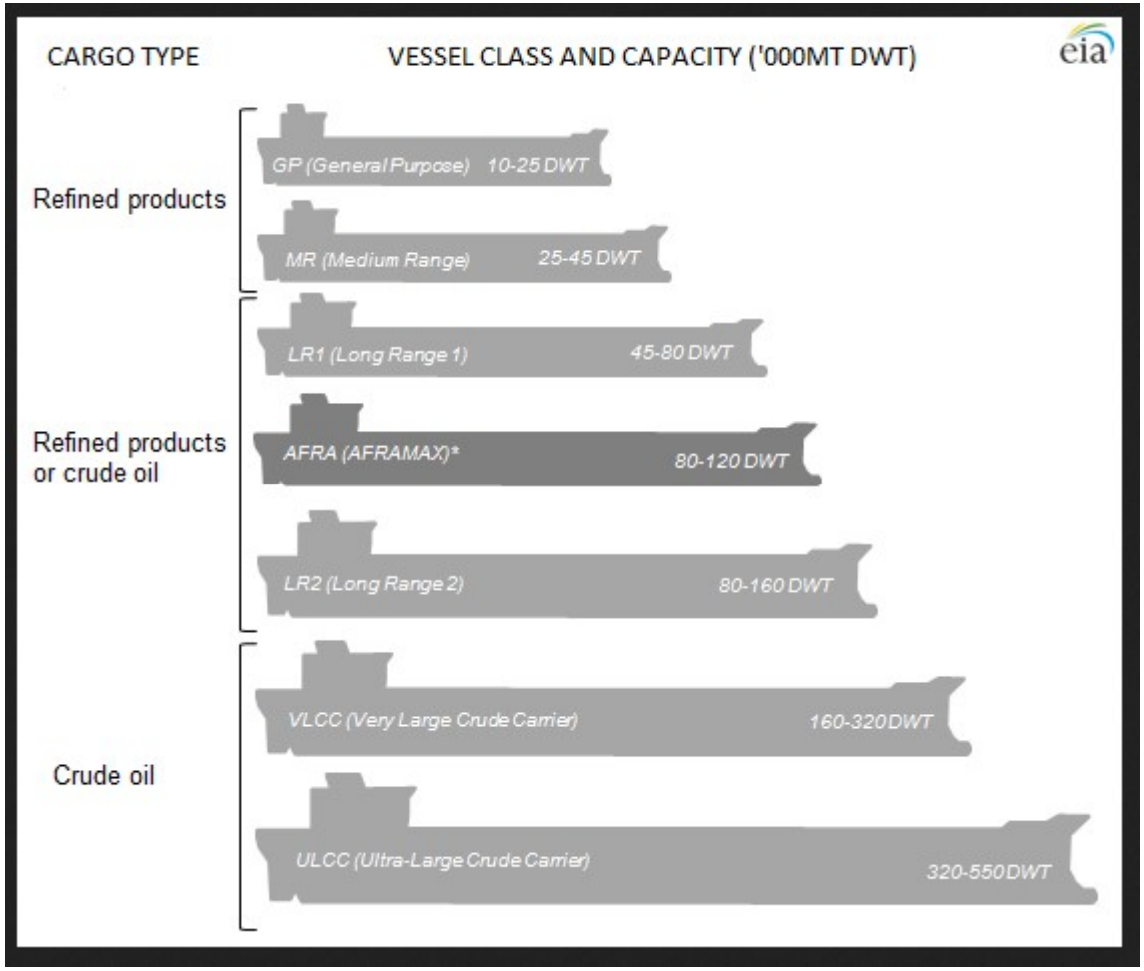

OOCL
OOCL
HAMBURG

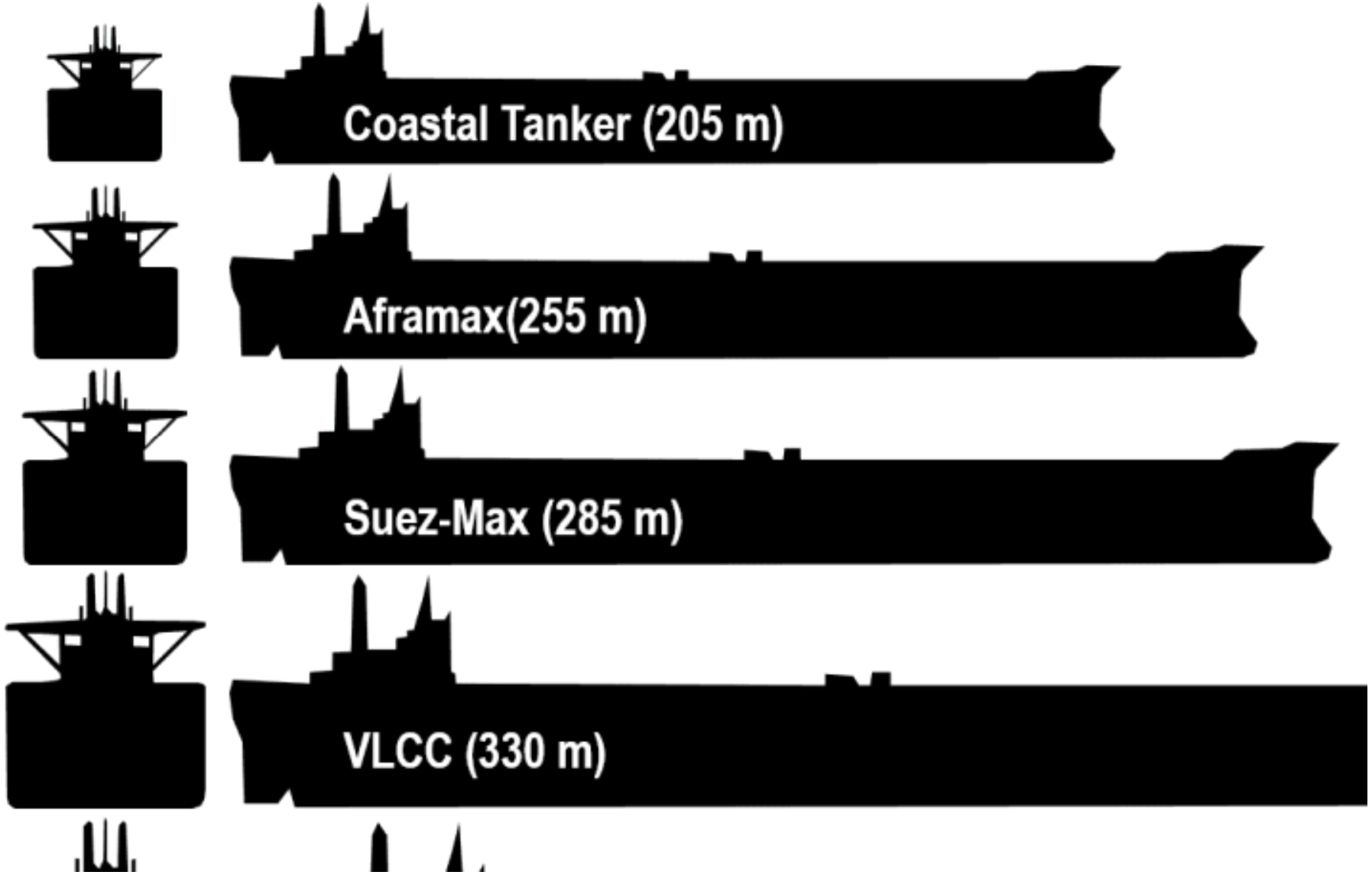

tex
tex

SHIP AHOY

- DIFFERENT TYPES, SHAPES & SIZES OF SHIPS
- CARRY DIFFERENT TYPES OF CARGO
- LARGE SHIPS - MORE CARGO –MORE VALUE
- FAST SHIPS- MORE AREA COVERED, LESS REACTION TIME FOR EMERGENCY
- DEEP SHIPS – LESS BOTTOM CLEARANCE- < 2 metres
- WHILE GOVERNMENT ENACTING LAW THAT VEHICLES MORE THAN 15 YEARS NEED TO BE SCRAPPED
- AGE OF SHIPS – UPTO 30 YEARS .
- OLD SHIPS MAY NOT BE COMPATIBLE WITH NEW HARDWARE /SOFT WARE ETC

TANKERS


CARGO TYPE
VESSEL CLASS AND CAPACITY ('000MT DWT)
eia
Refined products
GP (General Purpose) 10-25 DWT
MR (Medium Range) 25-45 DWT
Refined products or crude oil
LR1 (Long Range 1) 45-80 DWT
AFRA (AFRAMAX)* 80-120 DWT
LR2 (Long Range 2) 80-160 DWT
Crude oil
VLCC (Very Large Crude Carrier) 160-320 DWT
ULCC (Ultra-Large Crude Carrier) 320-550 DWT


Coastal Tanker (205 m)
Aframax(255 m)
Suez-Max (285 m)
VLCC (330 m)


ULCC
4 LAKH TONS
FLOATING BOMB
TIME TO STOP-
MOMENTUM
TURNING SLOW
HELLESPONT ALHAMBRA
MAJURO


LNG /LPG CARRIER
FLOATING BOMB

23,000+ CONTAINERS


GENERAL CARGO SHIP
Large holds

OIL RIGS IN THE EEZ


FREEDOM OF THE SEAS

THE SEA FARER

SMALL CREW SIZE – TO SAVE ON COSTS

LONG WORKING HOURS

MULTI –NATIONAL

SHORT CONTRACTS- 6 MONTHS

IMO MANDATED COURSES

FAR FROM FAMILY -BOREDOM, FATIGUE

ROUGH WEATHER , CYCLONES

LIMITATIONS IN CYBER SECURITY –LIKE OTHERS

KEEP CHANGING SHIPS AND COMPANIES- LOYALTY

INDIANS FORM ABOUT 10% OF WORLDS SEAFARERS

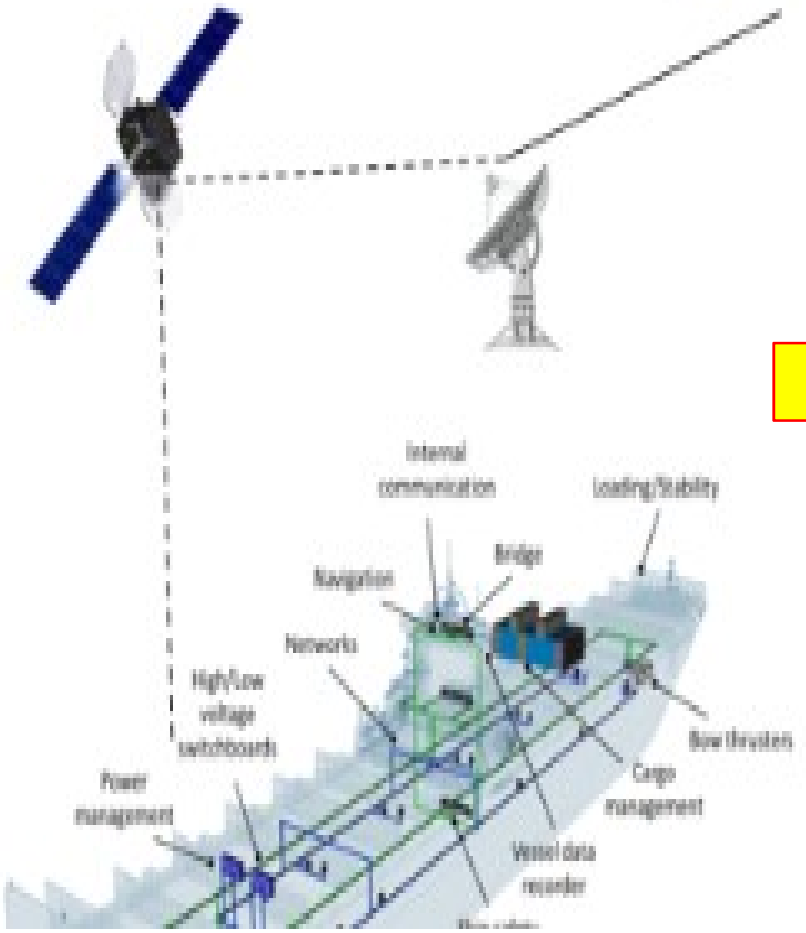
WHY SHIPPING IS VULNERABLE

- MOBILE PLATFORMS – COMMUNICATION
- DIGITIZATION & INCREASING CONNECTIVITY TO 'SHORE SIDE' TO IMPROVE EFFICIENCY
- AUTOMATION - to reduce crew size
- REMOTE ACESS CAPABILITY
- CONSTANT DATA STREAM
- CONVERGENCE OF IT SYSTEMS AND OT SYSTEMS
- COVID-19 & LOCKDOWN HAS INCREASED ON LINE WORK
- VULNERABLE

DIGITIZATION/ CONNECTIVITY /AUTOMATION-SHIP SYSTEMS
SHIP -SHORE DATA STREAM

- ENGINE PERFORMANCE MONITORING
- REMOTE DIAGNOSTICS
- MAINTENANCE AND SPARE PARTS MANAGEMENT
- CARGO AND CONTAINER TRACKING AND MANAGEMENT, LOADING AND UNLOADING, AND STOWAGE PLANNING
- CRANE AND PUMP MANAGEMENT
- MONITORING OF SYSTEMS FOR ADHERENCE TO ENVIRONMENTAL REGULATIONS AND REPORTING
- VOYAGE PERFORMANCE MONITORING
- LIFE OF CAPTAIN & CREW – OFTEN DIFFICULT BECAUSE OF REMOTE MONITORING

On-shore organization

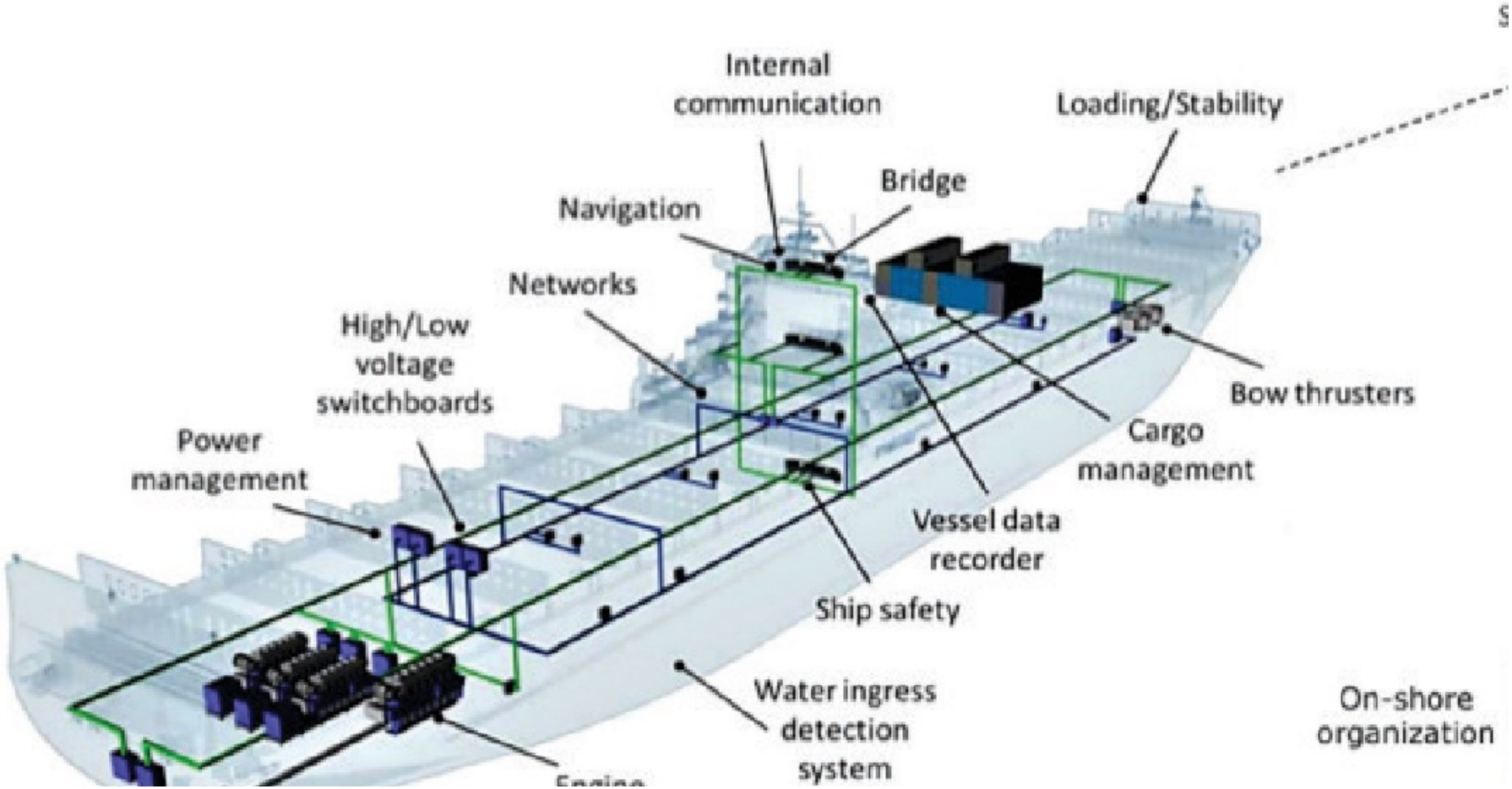


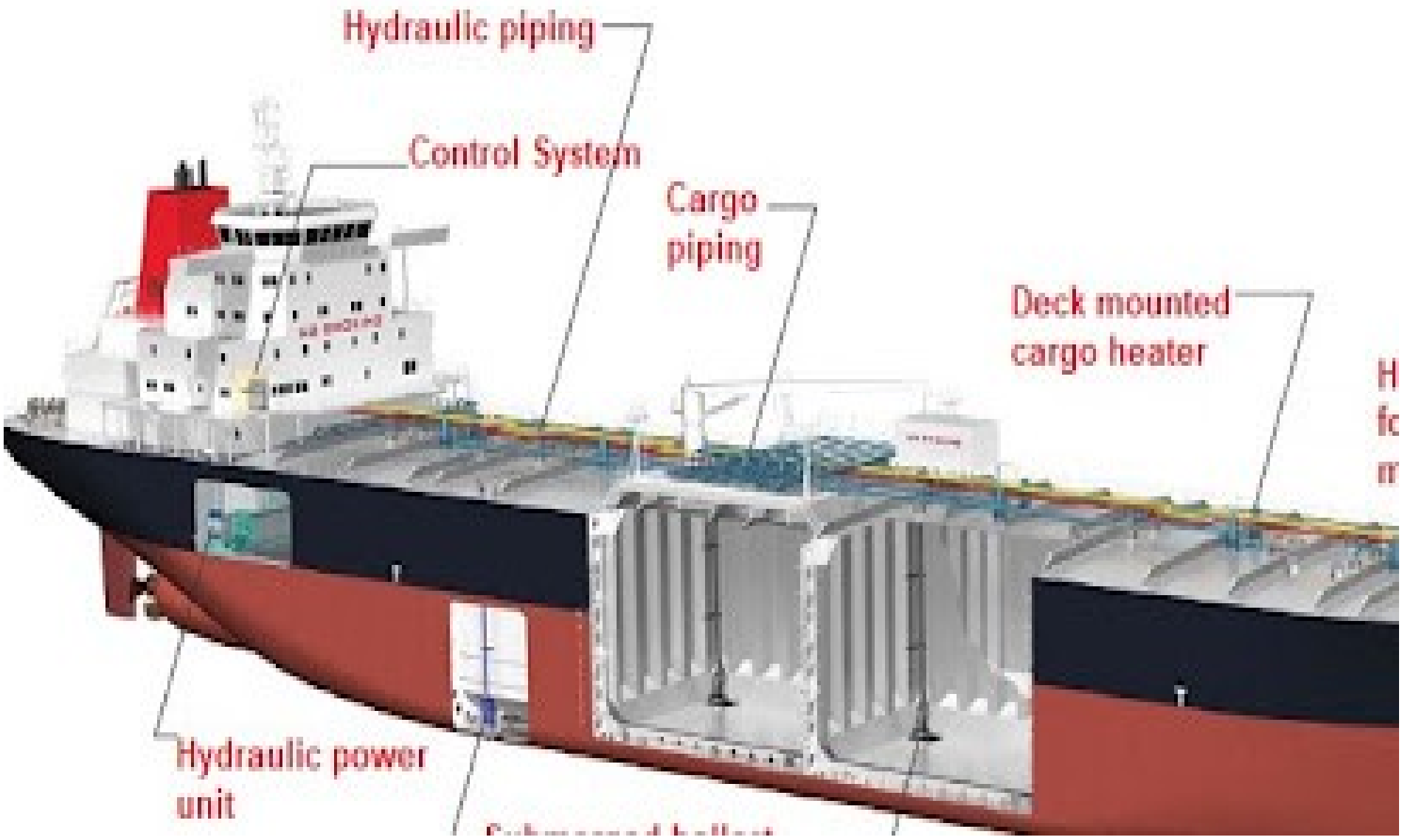
Information Technology (IT)

- Administration, accounts, crew lists, etc.
- Planned maintenance
- Spares management and requisitioning
- Electronic manuals and certificates
- Permits to work
- Charter party, notice of readiness, etc.

Operation Technology (OT)

- PLCs, SCADA
- On-board measurement and control
- ECDIS, GPS
- Remote support for engines


Internal communication
Loading/Stability
Bridge
Navigation
Networks
High/Low voltage switchboards
Power management
Bow thrusters
Cargo management
Vessel data recorder
Ship safety
Water ingress detection system
On-shore organization


Hydraulic piping
Control System
Cargo
piping
Deck mounted
cargo heater
Hydraulic power
unit

CYBER VULNERABILITIES

- OBSOLETE AND UNSUPPORTED OPERATING SYSTEMS
- UNPATCHED SYSTEM SOFTWARE
- OUTDATED OR MISSING ANTIVIRUS SOFTWARE AND PROTECTION FROM MALWARE
- INADEQUATE SECURITY CONFIGURATIONS AND BEST PRACTICES, INCLUDING INEFFECTIVE NETWORK MANAGEMENT AND THE USE OF DEFAULT ADMINISTRATOR ACCOUNTS AND PASSWORDS
- SHIPBOARD COMPUTER NETWORKS, WHICH LACK BOUNDARY PROTECTION MEASURES AND SEGMENTATION OF NETWORKS
- SAFETY CRITICAL EQUIPMENT OR SYSTEMS ALWAYS CONNECTED WITH THE SHORE SIDE
- INADEQUATE ACCESS CONTROLS TO CYBER ASSETS, NETWORKS ETC FOR THIRD PARTIES INCLUDING CONTRACTORS AND SERVICE PROVIDERS
- STAFF INADEQUATELY TRAINED AND/OR SKILLED TO MANAGE CYBER RISKS- UE OF PERSONAL DEVICES
- MISSING, INADEQUATE OR UNTESTED CONTINGENCY PLANS AND PROCEDURES.

TYPE OF ATTACKS

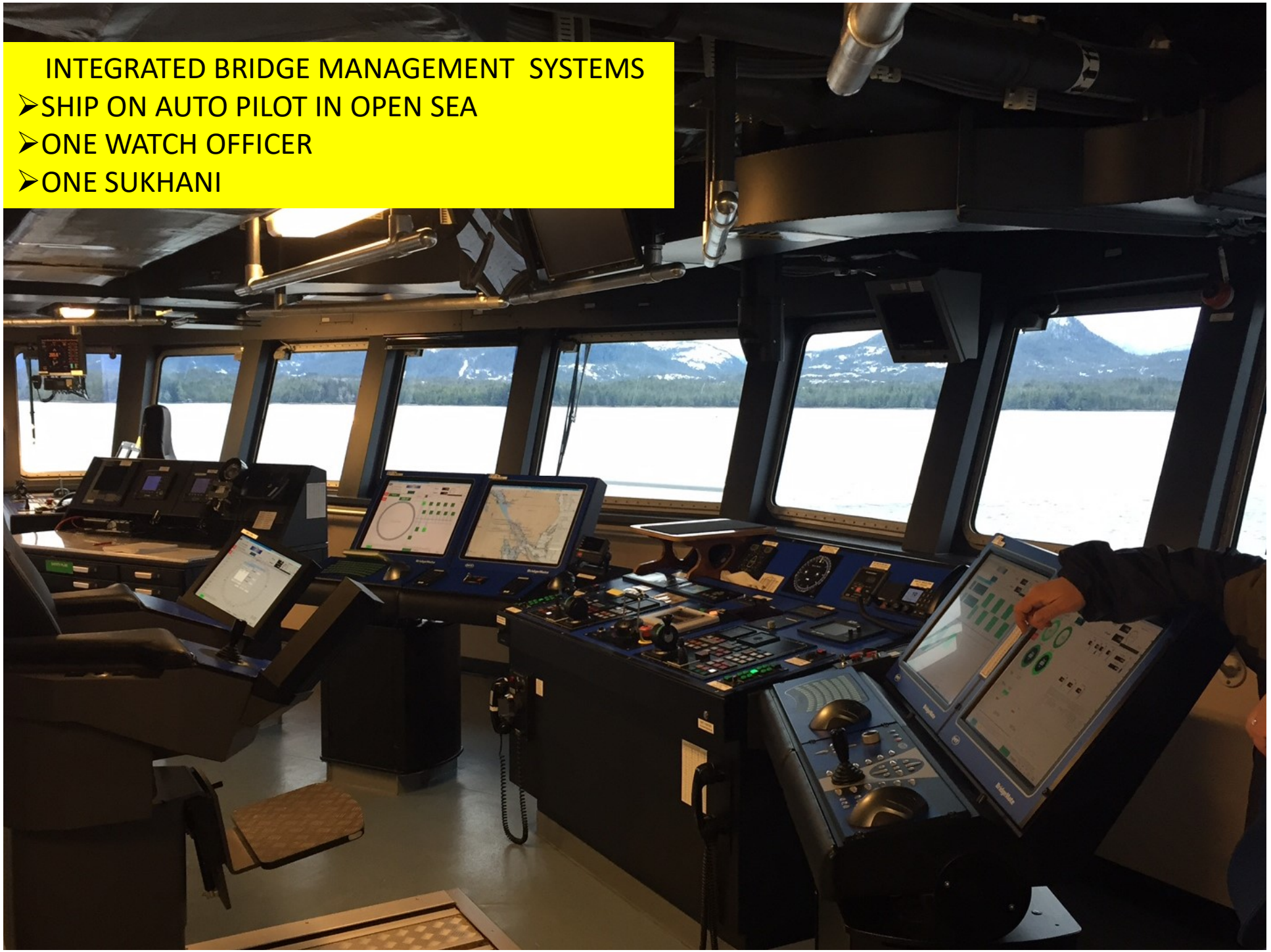
- MALWARE
- RANSOM
- PHISHING
- SOCIAL ENGINEERING
- BRUTE FORCE
- DENIAL OFF SERVICE
- MAN IN THE MIDDLE
- SUPPLY CHAIN
- SPOOFING

OPERATIONAL SYSTEMS

- GPS – GEOGRAPHIC POSITIONING SYSTEM
- PROVIDES INPUTS TO :
- ECDIS (ELECTRONIC CHART DISPLAY & INFORMATION SYSTEMS)
- RADAR
- ARPA (AUTOMATIC RADAR PLOTTING AID)
- ELECTRONIC NAVIGATION CHART (ENC)
- AIS (AUTOMATIC IDENTIFICATION SYSTEMS)
- DYNAMIC POSITIONING SYSTEMS (DPS)
- VDR (VOYAGE DATA RECORDER)
- GYRO SYSTEMS
- NAVIGATION –
- STEERING/DIRECTION- SHIP CAN BE MADE TURN INVOLUNTARILY
- INCREASE OR DECREASE SPEED
- INTEGRATED BRIDGE SYSTEMS

COMMUNICATIONS

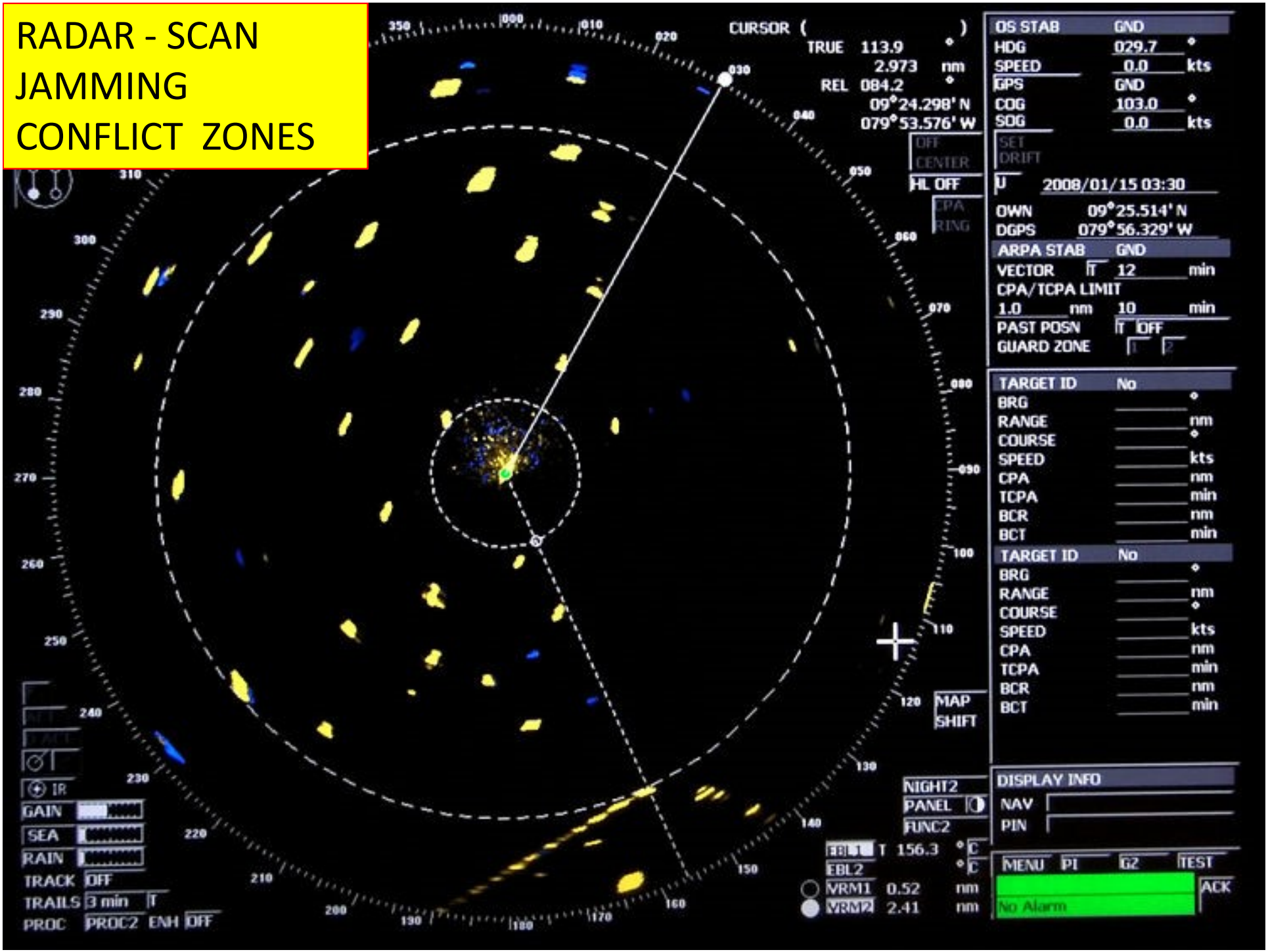
V/UHF
MF
HF
SATCOM


INTEGRATED BRIDGE MANAGEMENT SYSTEMS
➢SHIP ON AUTO PILOT IN OPEN SEA
➢ONE WATCH OFFICER
➢ONE SUKHANI

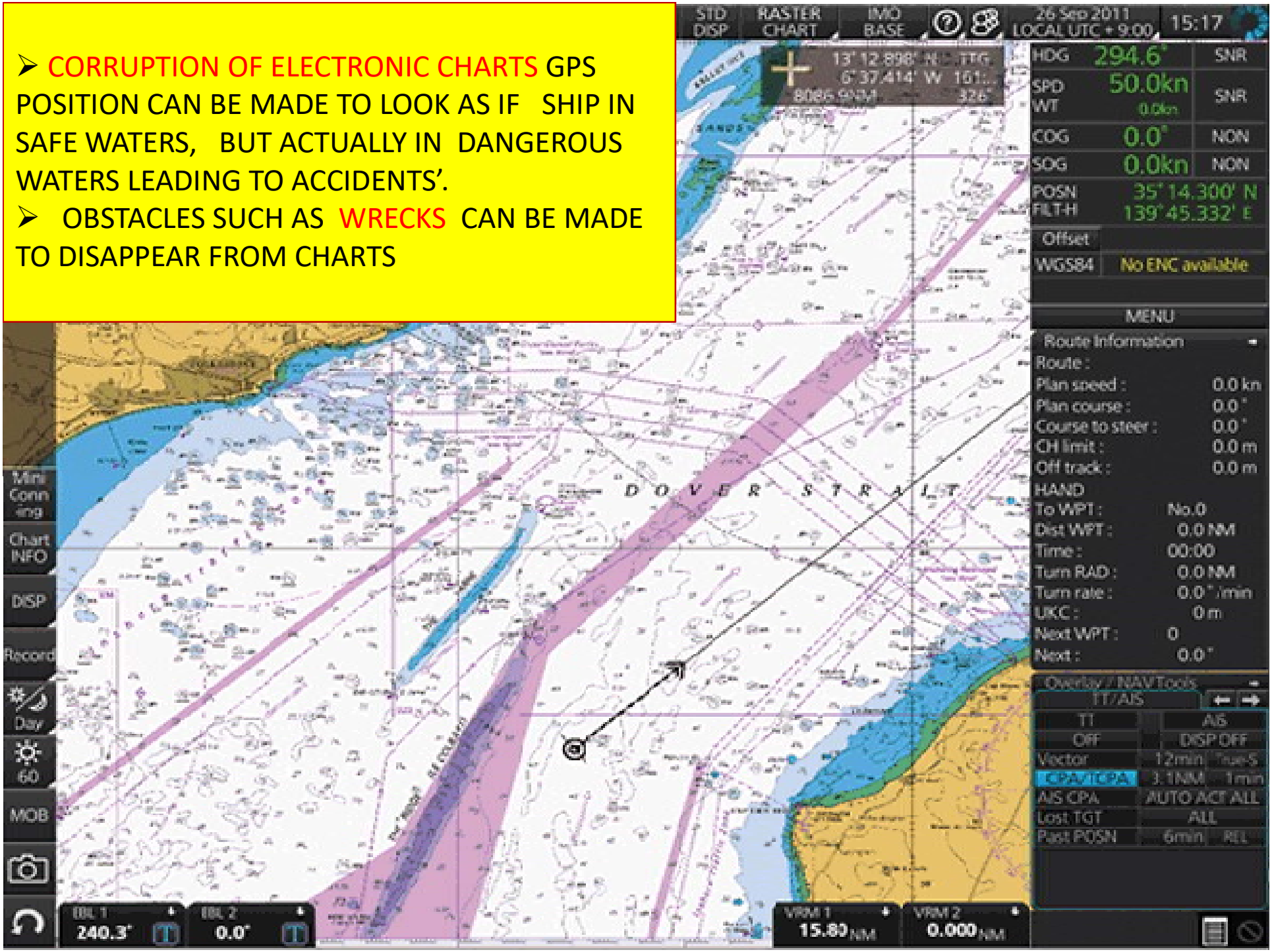
SPOOFING & JAMMING

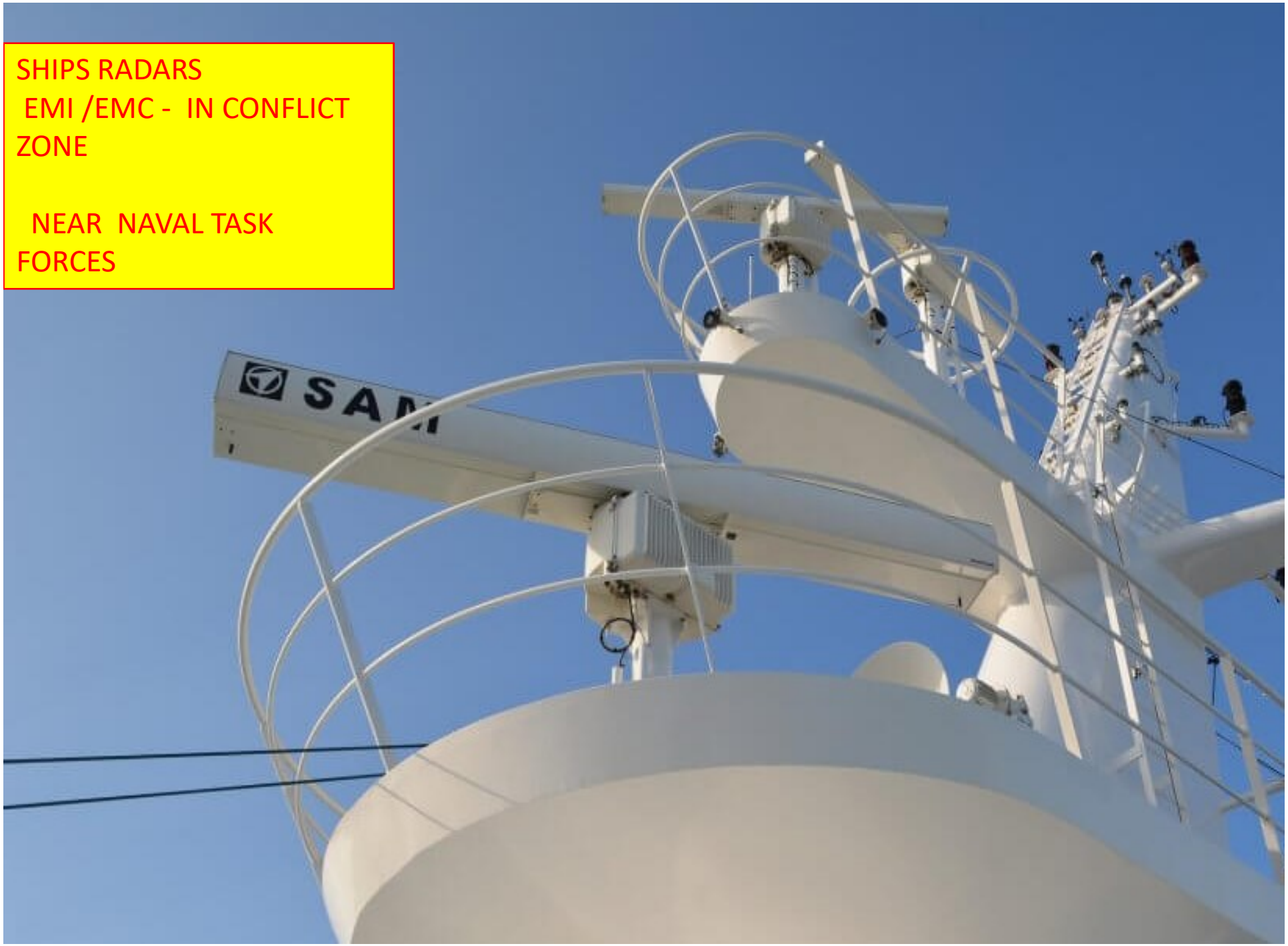
Adversaries may attempt to disrupt position, navigation and time solutions derived from GPS in one of two ways: **spoofing** (making a GPS receiver calculate a false position); and **jamming** (overpowering GPS satellite signals locally so that a receiver can no longer operate).

RADAR - SCAN
JAMMING
CONFLICT ZONES



- CORRUPTION OF ELECTRONIC CHARTS GPS POSITION CAN BE MADE TO LOOK AS IF SHIP IN SAFE WATERS, BUT ACTUALLY IN DANGEROUS WATERS LEADING TO ACCIDENTS'.
- OBSTACLES SUCH AS WRECKS CAN BE MADE TO DISAPPEAR FROM CHARTS




SHIPS RADARS
EMI /EMC - IN CONFLICT ZONE
NEAR NAVAL TASK FORCES
SAM

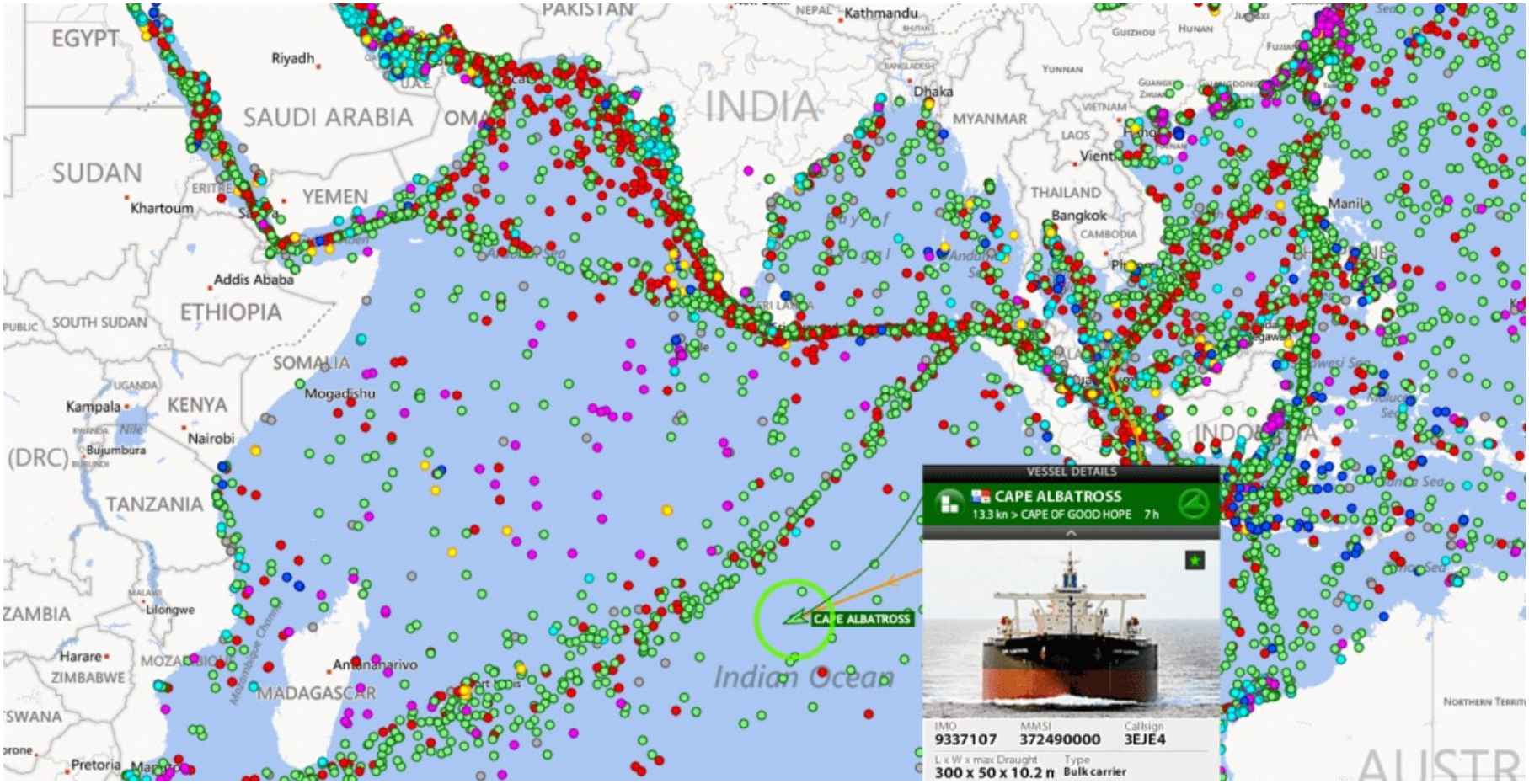
GPS

- GPS/NAVSTAR- US
- BEIDOU- CHINA
- GLASSNOSS- RUSSIA
- INDIA REGIONAL NAVIGATION SATELLITE SYSTEM (IRNSS)- NAVIK- INDIA

VULNERABILITY OF GPS

- LOW POWER OF SIGNAL STRENGTH
- INTERFERENCE/ JAMMING / SPOOFING
- TECH FAILURE - ATMOSPHERIC DISTURBANCE , MAGNETIC STORM ,
- THREE SATELLTES REQUIRED FOR TRIANGULATION
- COULD BE SWITCHED OFF IN TENSE SITUATIONS


AIS


EGYPT
Riyadh
SAUDI ARABIA
OMAN
PAKISTAN
NEPAL
Kathmandu
INDIA
Dhaka
MYANMAR
SUDAN
Khartoum
YEMEN
THAILAND
Bangkok
CAMBODIA
Manila
Addis Ababa
ETHIOPIA
SOUTH SUDAN
SOMALIA
Mogadishu
UGANDA
Kampala
KENYA
Nairobi
Bujumbura
(DRC)
TANZANIA
ZAMBIA
Lilongwe
Harare
ZIMBABWE
MADAGASCAR
Antananarivo
Indian Ocean
Pretoria
CAPE ALBATROSS
VESSEL DETAILS
CAPE ALBATROSS
13.3 kn > CAPE OF GOOD HOPE 7 h
IMO
9337107
MMSI
372490000
Callsign
3EJE4
L x W x max Draught
300 x 50 x 10.2 m
Type
Bulk carrier

The Shipborne Automatic Identification System (AIS) is a vessel tracking system capable of communicating navigation information automatically between AIS equipped vessels and coastal authorities. It is a collision avoidance system that gives information all the ships in your area, their speed and courses and how to contact them (name, callsign, MMSI). This information is publically broadcast on VHF radio which can be picked up by other ships

AIS

VULNERABILTY

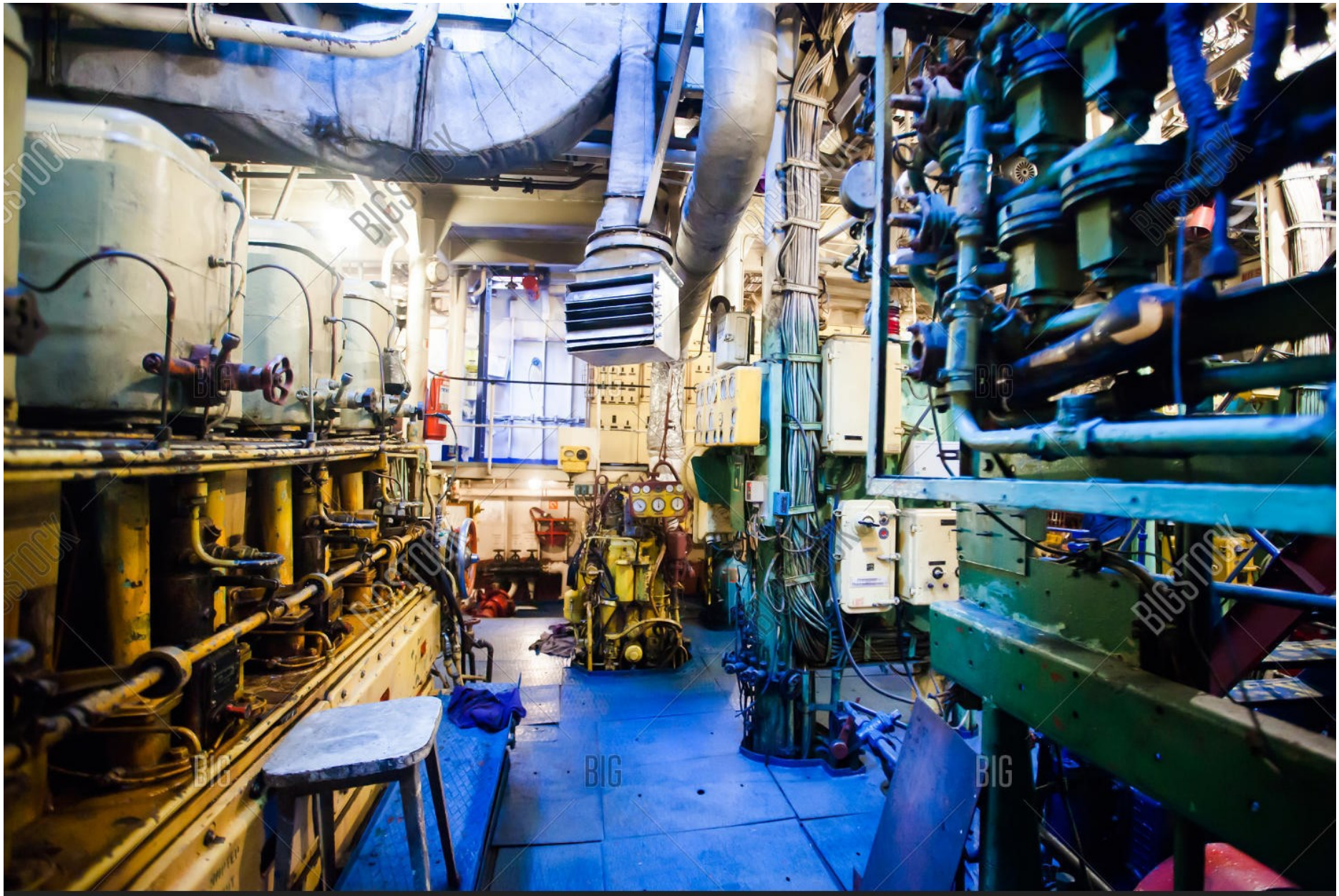
- MODIFICATION OF ALL SHIP DETAILS SUCH AS POSITION, COURSE, CARGO, FLAGGED COUNTRY, SPEED, NAME & MMSI
- CREATION OF FAKE VESSELS
- CREATE AND MODIFY AID TO NAVIGATIONS , SUCH AS BUOYS AND LIGHTHOUSES.

INCIDENT

in June 2017, when a GPS spoofing attack involving over 20 ships in the Black Sea made them “disappear.” Instead of showing actual positions, ships were being shown 25 to 30 miles away at Gelendzhik airport. When one ship operator radioed the other vessels, it was confirmed that there was an issue with everyone’s GPS. GPS spoofing can deliver potentially catastrophic consequences: ships could be directed off course and criminals could take advantage to steal precious cargo.

SHIPS MACHINERY

- PROPULSION MACHINERY
- GENERATORS
- COMPRESSRS
- CARGO PUMPS
- FIRE FIGHTING
- BOW THRUSTERS
- REFRIGERATION
- AC
- STABILIZERS
- STEERING PUMPS


BIGSTOCK
Image ID: 156469856
bigstock.com

AUTOMATED ENGINE CONTROL ROOM

ENGINE ROOMS , MACHINERY NOT MANNED

SHIP SYSTEMS

- PROPULSION- THROTTLE CAN BE MADE TO BECOME STUCK eg '*FULL AHEAD POSITION* ' SO SHIP UNABLE TO STO*P*
- BALLAST SYSTEMS – HIGH CAPACITY PUMPS & VALVES CAN BECOME STUCK LEADING TO FLOODING /SHIP STABILITY PROBLEMS
- CARGO SYSTEMS – CRUDE OIL& GAS

EFFECTS

- BUSINESS / FINANCIAL /COMMERCIAL LOSS
- TAMPERING WITH MANIFEST /CONTAINER RFID

- SAFETY OF SHIP
- COLLISION
- GROUNDING
- FLOODING
- SINKING
- MARINE POLLUTION

- LOSS OF REPUTATION
- INCREASE IN INSURANCE COST
- LOSS OF LIFE & LIMB

➢CAN BE MADE TO:

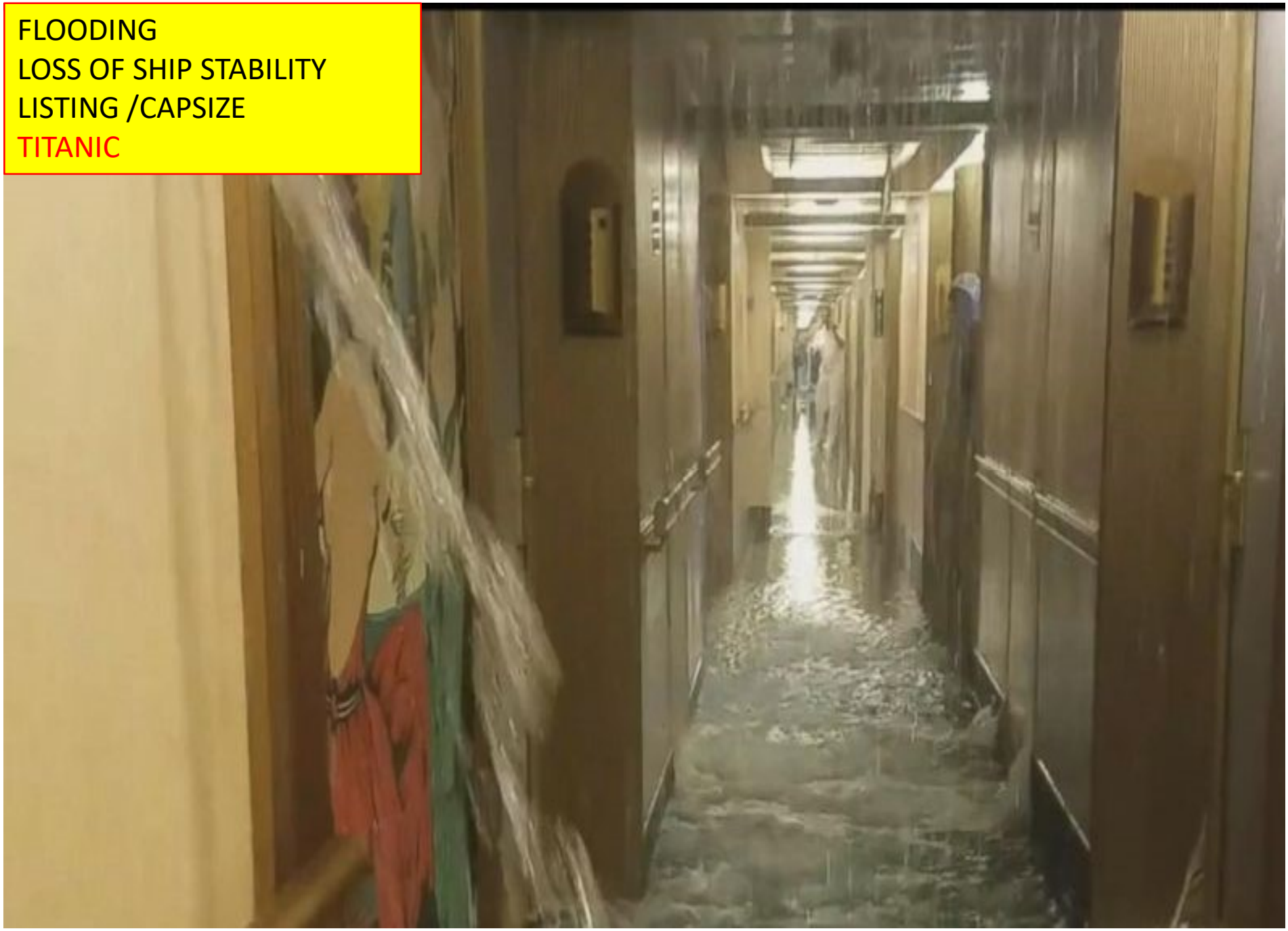
•PUMP IN WATER TO CONTAMINATE CRUDE

•PUMP OUT CRUDE TO SEA TO CAUSE POLLUTION

•COLLIDE WITH OTHER SHIPS OR HARBOUR INFRA -STRUCTURE


Leak
UASC
UASC

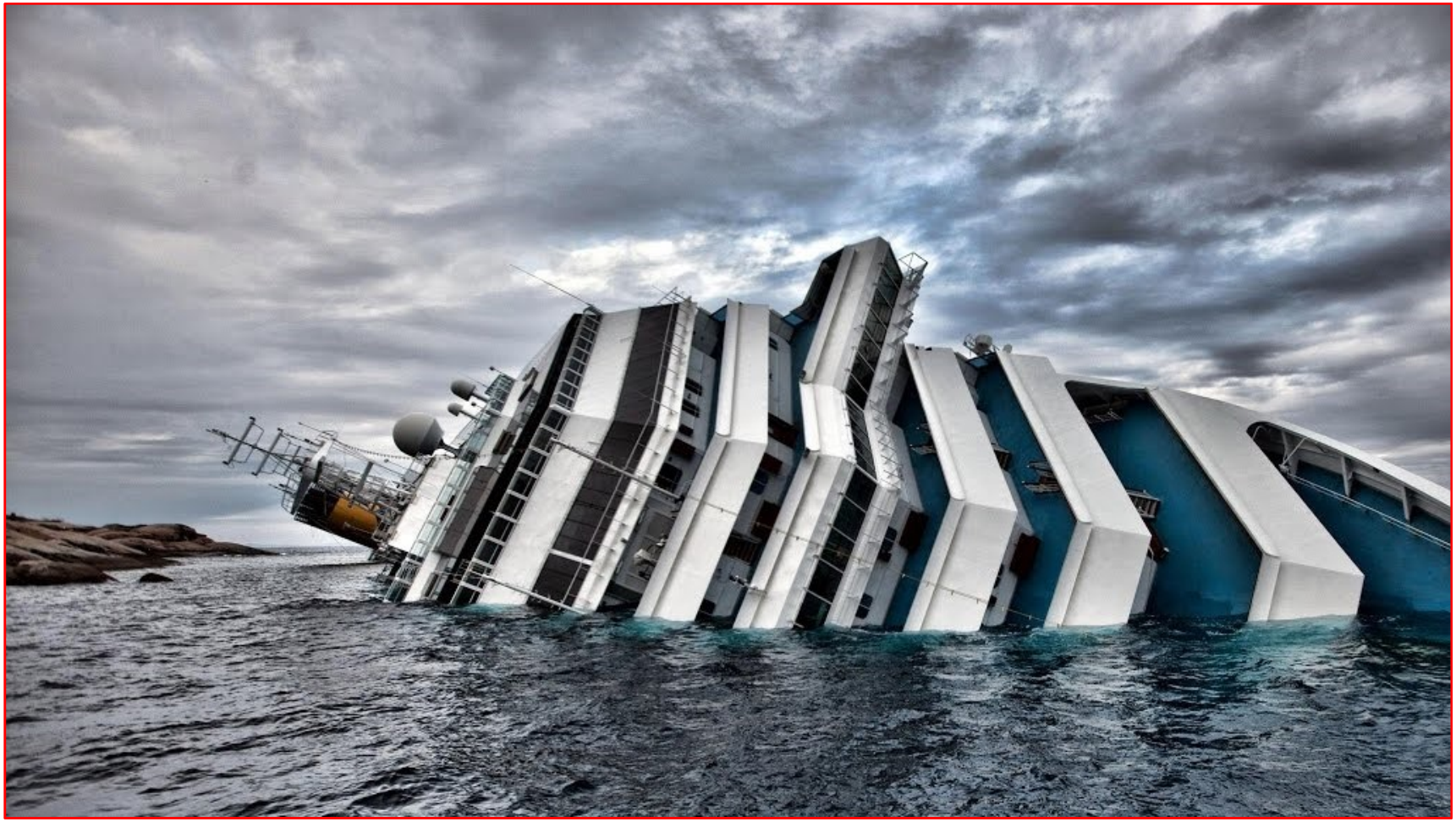
FLOODING
LOSS OF SHIP STABILITY
LISTING /CAPSIZE
TITANIC



SHIP MADE TO GO AGROUND


COLLISION

COSTA CONCORDIA DISASTER



CRUISE SHIPS

- LARGE NO OF GUESTS & CREW : 3000 -5000
- FOREIGNERS OF VARIOUS NATIONALITIES
- PASSENGER DATA CAN BE STOLEN
- PROGRAMME CAN BE CHANGED/DELAYED
- CAUSING LOSS IN PASSENGER ITNERARY , FLIGHT RESERVATIONS ETC
- SHIPS TOP HEAVY , LARGE SPACES INSIDE LIKE SEVERAL RESTAURANTS, THEATRES, BARS MAKE IT VULNERABLE

OIL SPILL - MARINE POLLUTION

SHIP IN DAVY JONE’S LOCKER

SUEZ THROMBOSIS

SUEZ THROMBOSIS - EVERGREEN INCIDENT -COULD BE RECREATED BY HACKERS

HARBOURS WITH NARROW CHANNEL

- NEW MANGALORE
- KOCHI
- VISHAKAPATNAM
- HACKERS CAN BE BLOCK IT BY SINKING A SHIP
- ECONOMIC / ENVIRONMENTAL TERRORISM
- *GHAZI INCIDENT -1971 WAR*

PORTS


HMM

TAMPERING WITH CONTAINERS

- DUE LARGE NO OF CONTAINERS
- LOADING IS COMPUTERIZED
- 'FIRST IN - LAST OUT' POLICY
- HACKING CAN CHANGE LOADING SEQUENCE
- MANIFEST CAN BE CHANGED
- RFID NOS CAN BE TAMPERED
- WHEN SHIP ARRIVES IN NEXT PORT , THE CONTAINERS REQUIRED TO BE UNLOADED ARE DEEP DOWN & NOT ACCESSIBLE
- MANIFEST CORRUPTED
- CHAOS IN PORTS
- LONG LINE OF TRUCKS
- DELAYS LEADING TO FINANCIAL LOSS

MAY 2020

ISRAEL BROUGHT SHAHID RAJAEE PORT IN BANDAR ABBAS TO STANDSTILL WITH CYBER ATTACK .PORT OPS FOR WERE HALTED FOR SEVERAL DAYS . LONG LINE OF TRUCKS SEEN OUT SIDE THE PORT

Secret files show alleged Iranian plans to sink ships using cyberattacks

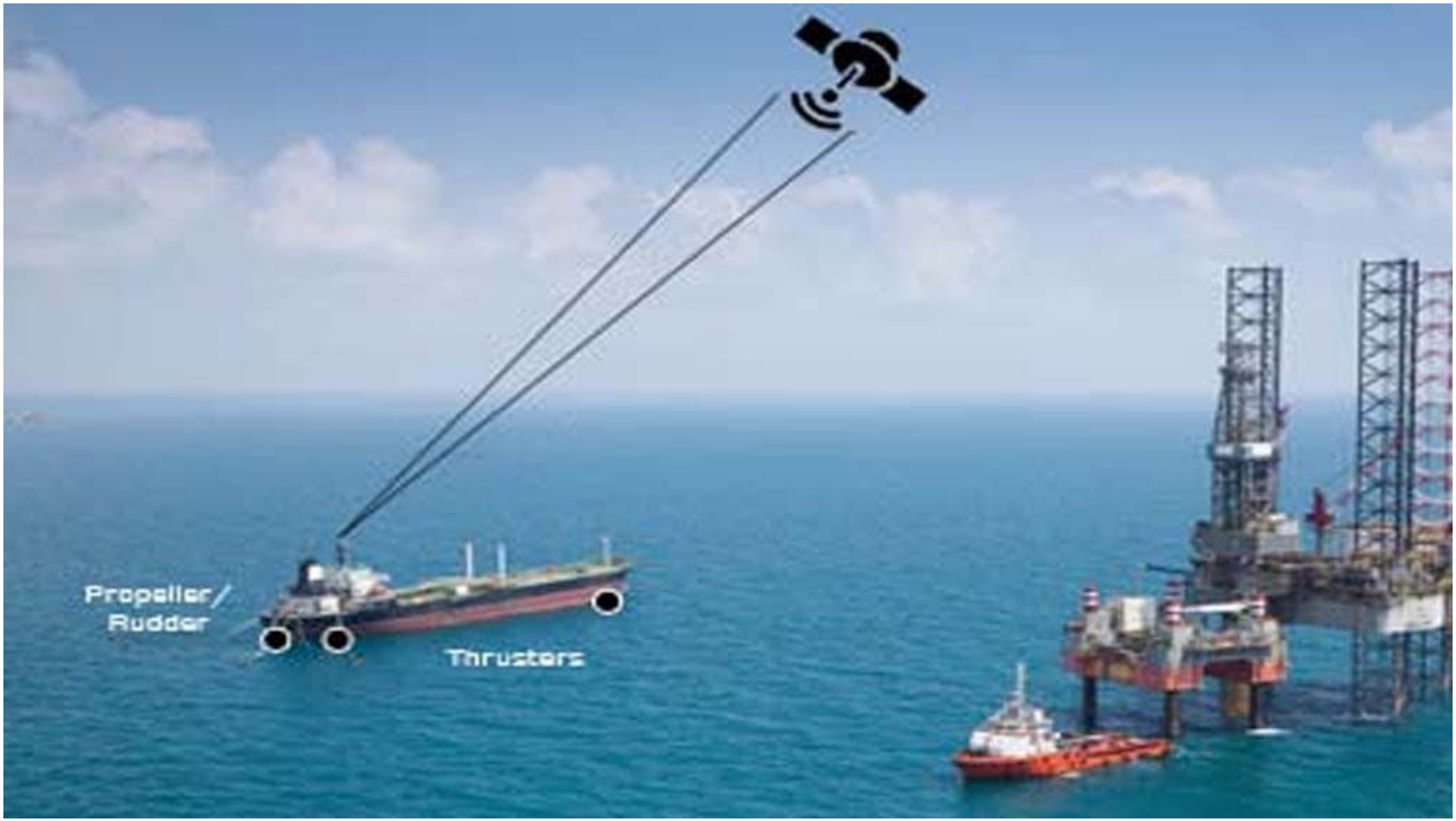
Iranian Revolutionary Guard documents obtained by cyber wafare name Israel, US, UK and others as potential targets; also say attacks could be used to blow up fuel pump at gas station

By **TOI STAFF**28 July 2021, 9:14 am

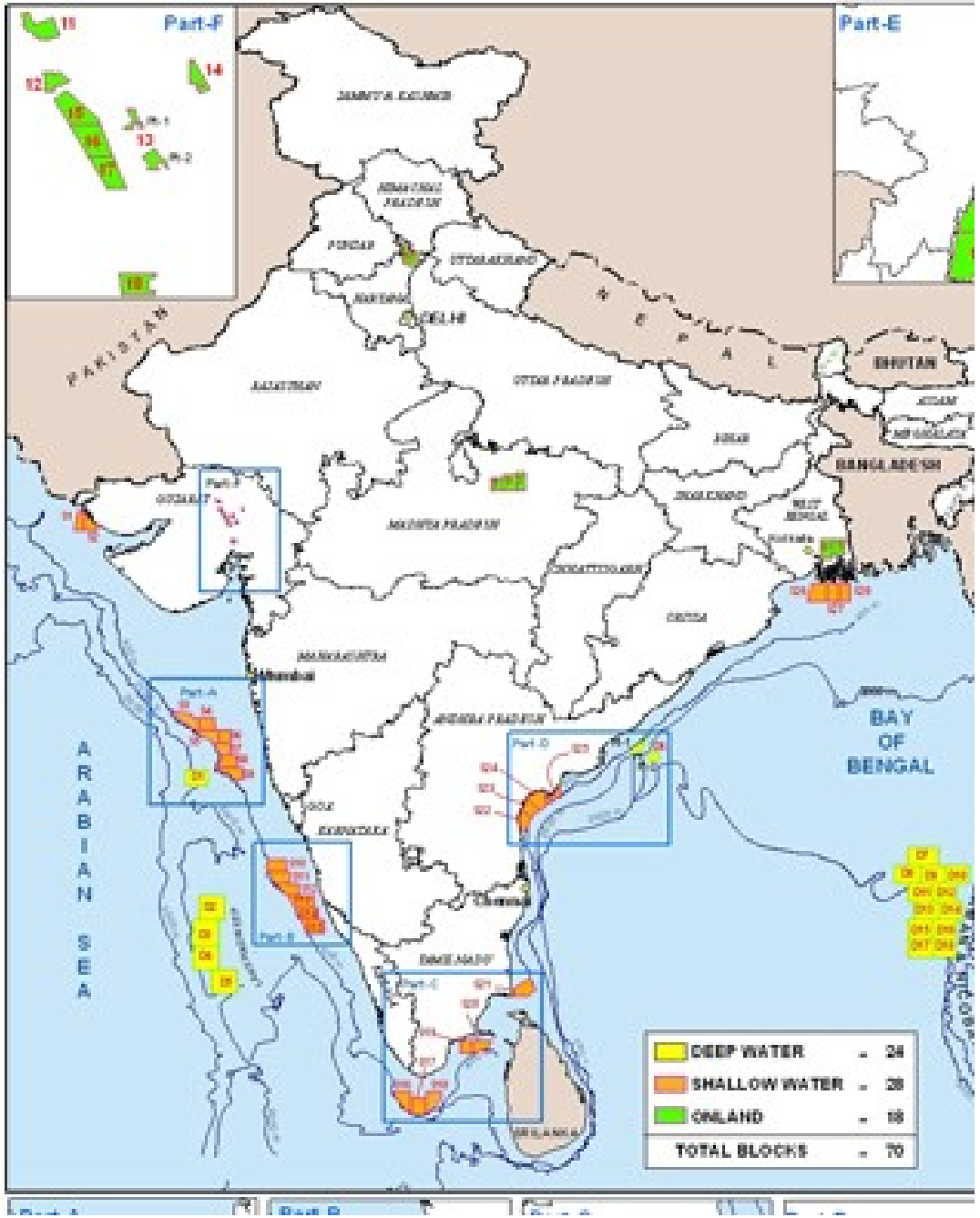
TIMES OF ISRAEL

US – SKY NEWS

OFF SHORE OIL& GAS RIG



EXPLORATION BLOCKS ON OFFER UNDER NEW EXPLORATION LICENSING POLICY - EIGHTH ROUNI



OUR RIG TYPES

Drillship
Operates at water depths of:
500 - 3,650 meters

Semi-submersible
Operates at water depths of:
50 - 3,000 meters

Ultra Harsh Environment Jack-up
Operates at water depths of:
21 -150 meters

High Efficiency Jack-up
Operates at water depths of:
21 -106 meters

Drilling Barge
Operates at water depths of:
5 - 50 meters

OIL RIGS

- RIGS/ SUPPORT VESSELS –DPS
- DYNAMIC POSITIONING SYSTEM –GPS FEED –COLLISION WITH RIG-FIRE
- BALLAST - CRITICAL VALVES AND HIGH END PUMPS – TAMPERED TO TILT THE RIG –RENDER NON –OPS

INCIDENT

A reported incident of spoofing involved hackers successfully tilting the floating oil rig which resulted in shutting its operations.

It took 19
days to make it seaworthy again after computer malware were removed from the computers controlling the rig.

INCIDENT

On May 7 , 2021 , a pipeline system carrying almost half the fuel used on the east coast of the United States was crippled by a major cyber attack. The five-day shutdown of the Colonial Pipeline resulted in widespread fuel shortages and panic-buying as Virginia, North Carolina and Florida declared a state of emergency.

VULNERABILITY OF OIL GRID

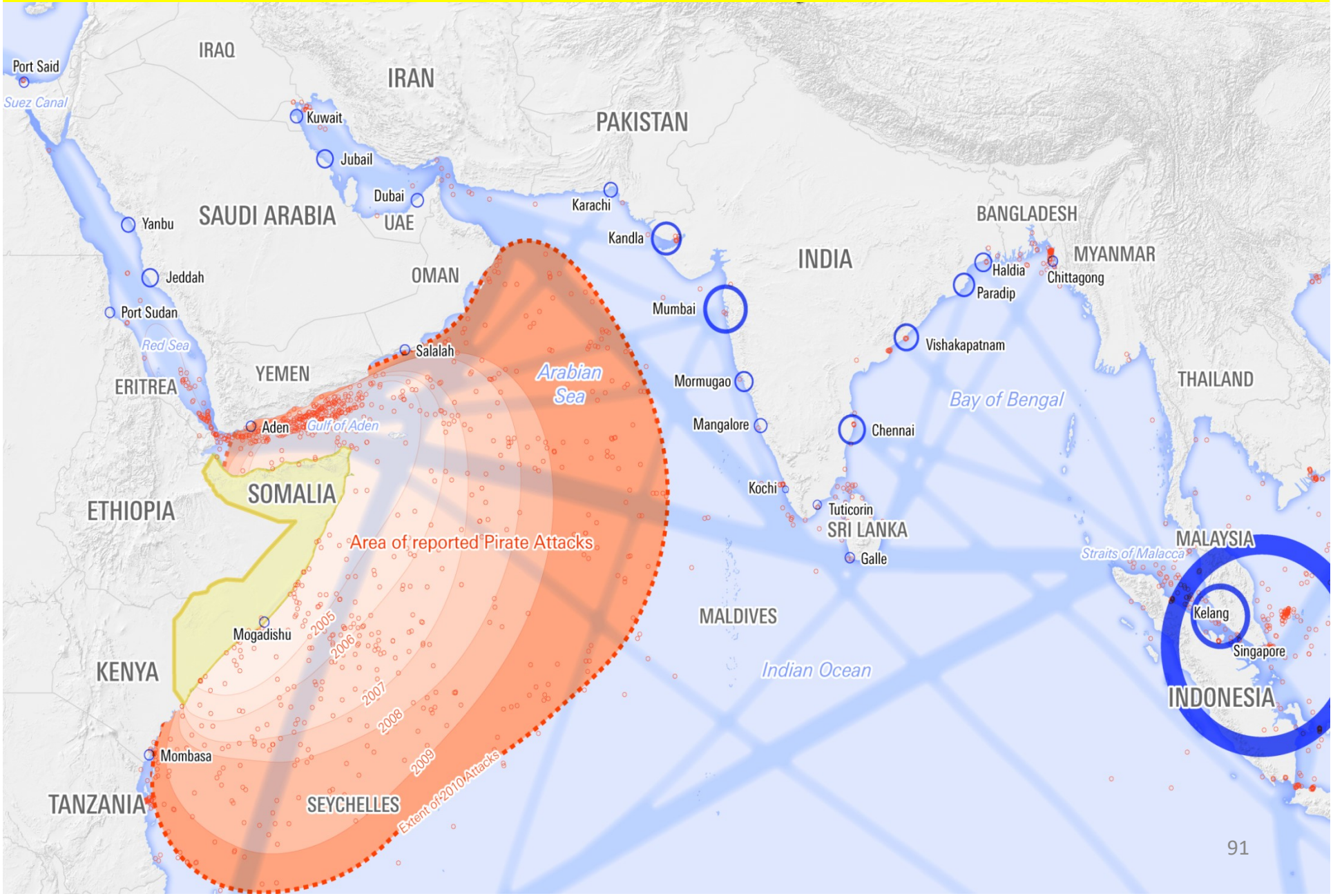

Nakhatrana
Tera
Naliya
Jakhau
Bhanada
Bhuj
Kukma
341
Kothara
Gadhsisa
Naranpar
Pantiya
8A
8A
Layja Mota
Koday
Mandvi
8A
Mundra
Gulf of Kutch
Okha
Mithapur
Chusna
Sikka
Vadinar
Motikhavdi
947
Varvala
Salaya
Dwarka
Khambhalia
947
Bhatiya
Bhadthar


FPMC 17
ALAM BISTARI


EAGLE COLUMBUS

- GULF OF KUTCH IS MOUTH OF NORTHERN OIL GRID
- ATLEAST 3-4 VERY LARGE CRUDE CARRIERS (VLCC) COME IN EVERY WEEK
- OIL PUMPED FROM KANDLA, SIKKA, SALAYA , VADINAR -FEED REFINERIES IN THE NORTH
- 3 REFINERIES IN GULF OF KUTCH
- SHIPS
- OIL HANDLING FACILITIES IN KANDLA / RELIANCE/ ESSAR
- SINGLE POINT MOORING
- VULNERABLE TO CYBER ATTACK
- HACKERS - STOP SUPPLY OF CRUDE - , REFINERIES WILL COME TO A GRINDING HALT
- NO FUEL AFTER 7-10 DAYS

PIRACY OFF SOMALIA



SOMALIA PIRATES

- ALONG WITH HACKERS -MONITOR SHIPPING & HARBOUR WEBSITES
- HACK INTO WEBSITES , ECDIS etc
- TO SEE ARRIVAL TIMES & CARGO MANIFEST
- TO SEE BLUE PRINT OF SHIP
- THEN ATTACK

INCIDENT

Somali pirates 'hand pick their shipping targets by tracking online the navigation track of the vessel' by breeching into the AIS and the Electronic Chart Display & Information System (ECDIS), a computer-based navigation information system which can be used as an alternative to traditional paper charts. This information was critical for the pirates to track the vessel and launch an attack.

MEDIA –REPORT

MOTIVATION & OBJECTIVES

MOTIVATION

- ACCIDENTAL ACTORS NO MALICIOUS MOTIVE BUT STILL END UP CAUSING UNINTENDED HARM THROUGH LACK OF KNOWLEDGE OR LACK OF CARE, eg BY INSERTING INFECTED USB IN ONBOARD IT OR OT SYSTEMS.

- ACTIVISTS (INCLUDING DISGRUNTLED EMPLOYEES) REVENGE, DISRUPTION OF OPERATIONS , MEDIA ATTENTION, REPUTATIONAL DAMAGE

- CRIMINALS FINANCIAL GAIN, COMMERCIAL ESPIONAGE, INDUSTRIAL ESPIONAGE

- OPPORTUNISTS- THE CHALLENGE, REPUTATIONAL GAIN, FINANCIAL GAIN ,STATES STATE SPONSORED ORGANISATIONS

- TERRORISTS POLITICAL/IDEALOGICAL GAIN EG (UN)CONTROLLED DISRUPTION TO ECONOMIES AND CRITICAL NATIONAL INFRASTRUCTURE - ESPIONAGE, FINANCIAL GAIN ,COMMERCIAL ESPIONAGE , INDUSTRIAL ESPIONAGE , COMMERCIAL GAIN
- ROGUE COUNTRIES – CHINA , RUSSIA, IRAN , NORTH KOREA

- PIRATES

MITIGATION

- **Identify the threat environment** to understand external and internal cyber threats to the ship
- **Identify vulnerabilities** by developing complete and full inventories of onboard systems and understanding the consequences of cyber threats to these systems
- **Assess risk exposure** by determining the likelihood and impact of a vulnerability exploitation by any external or internal actor
- **Develop protection and detection measures** to reduce the likelihood and the impact of a potential exploitation of a vulnerability
- **Establish prioritized contingency plans** to mitigate any potential identified cyber risk
- **Respond and recover from cyber incidents** using the contingency plan to ensure operational continuity

BIMCO

RISK ASSESSMENT

MITIGATION

- PHYSICAL SAFETY OF THE VESSEL IN ACCORDANCE WITH THE SHIP SECURITY PLAN (SSP)
- NETWORK PROTECTION, INCLUDING EFFICIENT SEGMENTATION
- INTRUSION DETECTION
- PERIODIC SCANNING AND TESTING OF VULNERABILITIES
- SOFTWARE WHITELIST
- ACCESS AND USER CONTROLS
- APPROPRIATE PROCEDURES REGARDING THE USE OF REMOVABLE MEDIA AND PASSWORD POLICIES
- STAFF AWARENESS OF THE RISKS AND FAMILIARITY WITH THE RELEVANT PROCEDURES.

MITIGATION

RELIANCE ON CREW

• SUFFICIENT AND CONTINUOUS TRAINING ON CYBER SECURITY • DEVELOPMENT OF A CYBER SECURITY POLICY

RELIANCE ON MANUAL BACK UP

•• CREW • PAPER CHARTS • GYRO/ MAGNETIC COMPASS , SHIPS LOG/RPM INDICATOR , CELESTIAL NAVIGATION , TERRESTRIAL NAVIGATION

VESSELS MUST BE TREATED AS ANY OTHER NETWORK

• SECURITY AUDITS • PENETRATION TESTING • PHYSICAL SECURITY ASSESSMENTS

INCIDENT RESPONSE

• DEVELOPMENT OF CONTINGENCY PLANS

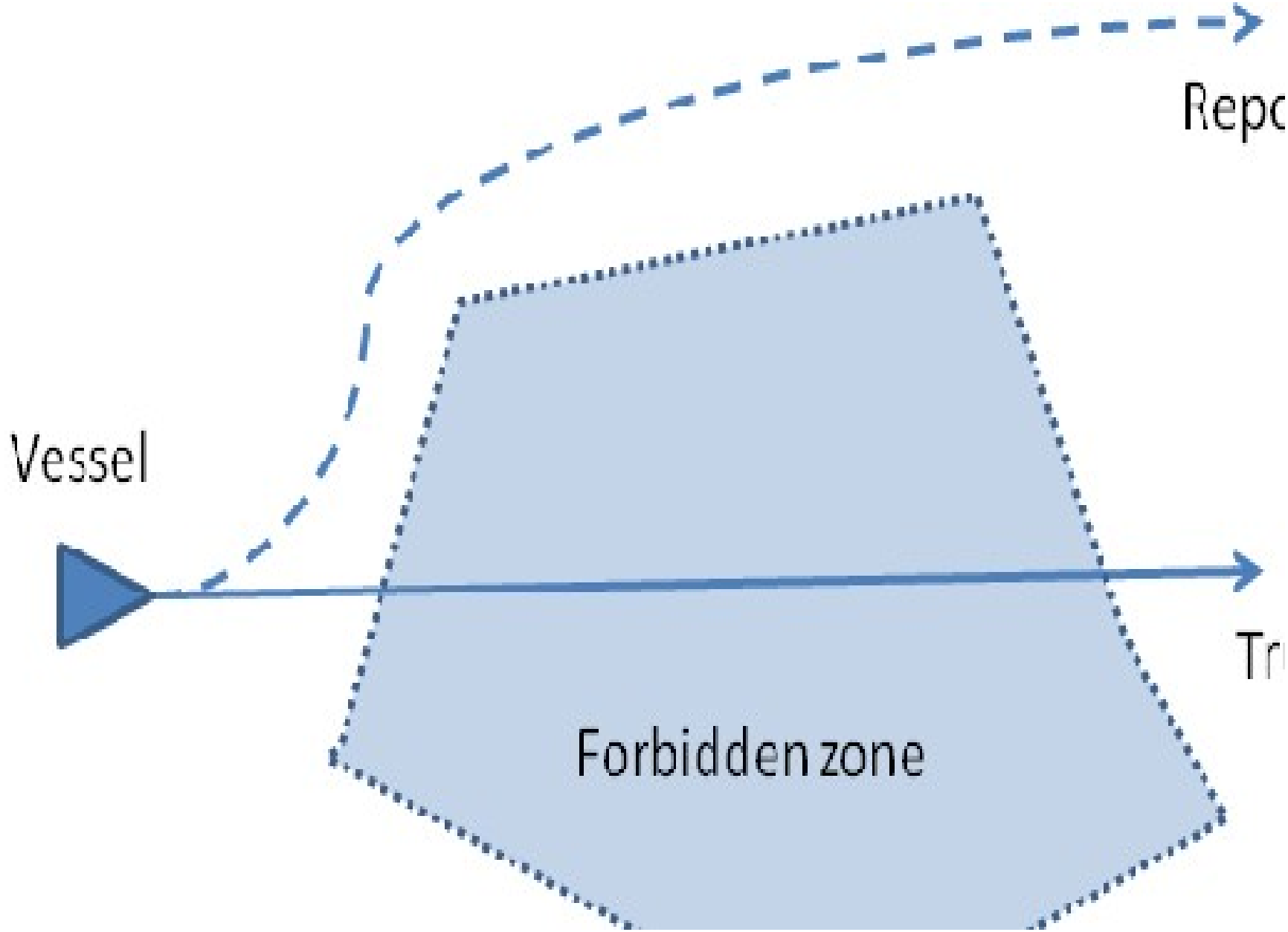
INCIDENT

Danish shipping giant Maersk (A.P. Møller-Maersk) fell victim to NotPetya in June 2017. While Maersk lost most of its data, applications, over 49,000 laptops and almost half of their servers, the computers on their actual ships were spared. However, the terminals' software designed to receive the Electronic Data Interchange files from those ships had been wiped entirely.

INCIDENT

Smugglers hacked into the port cargo handing data and were able to locate the containers with drugs which were pilfered without detection. Interestingly, the smugglers even managed to tamper the cargo manifest and deleted the data of the shipment.

Fishing vessel crew may turn off its AIS broadcast for a variety of legitimate reasons, but this behavior may indicate that **a vessel is hiding its location and identity to conceal illegal activities like fishing** in no-take protected areas or entering another country's waters without authorization


Repc
Vessel
Tr
Forbidden zone

INTERNATIONAL AND NATIONAL REGULATIONS

IMO RESOLUTION

FLAG STATE AUDIT

DG SHIPPING

INDIAN REGISTER OF SHIPPING (IRS)

NSCS – CYBER SECURITY ADVISER

DEFENCE FORCES - DEFENCE CYBER AGENCY

–CYBER SECURITY WARFARE OFFICERS

NATIONAL CYBER SECURITY POLICY

CERT –IN

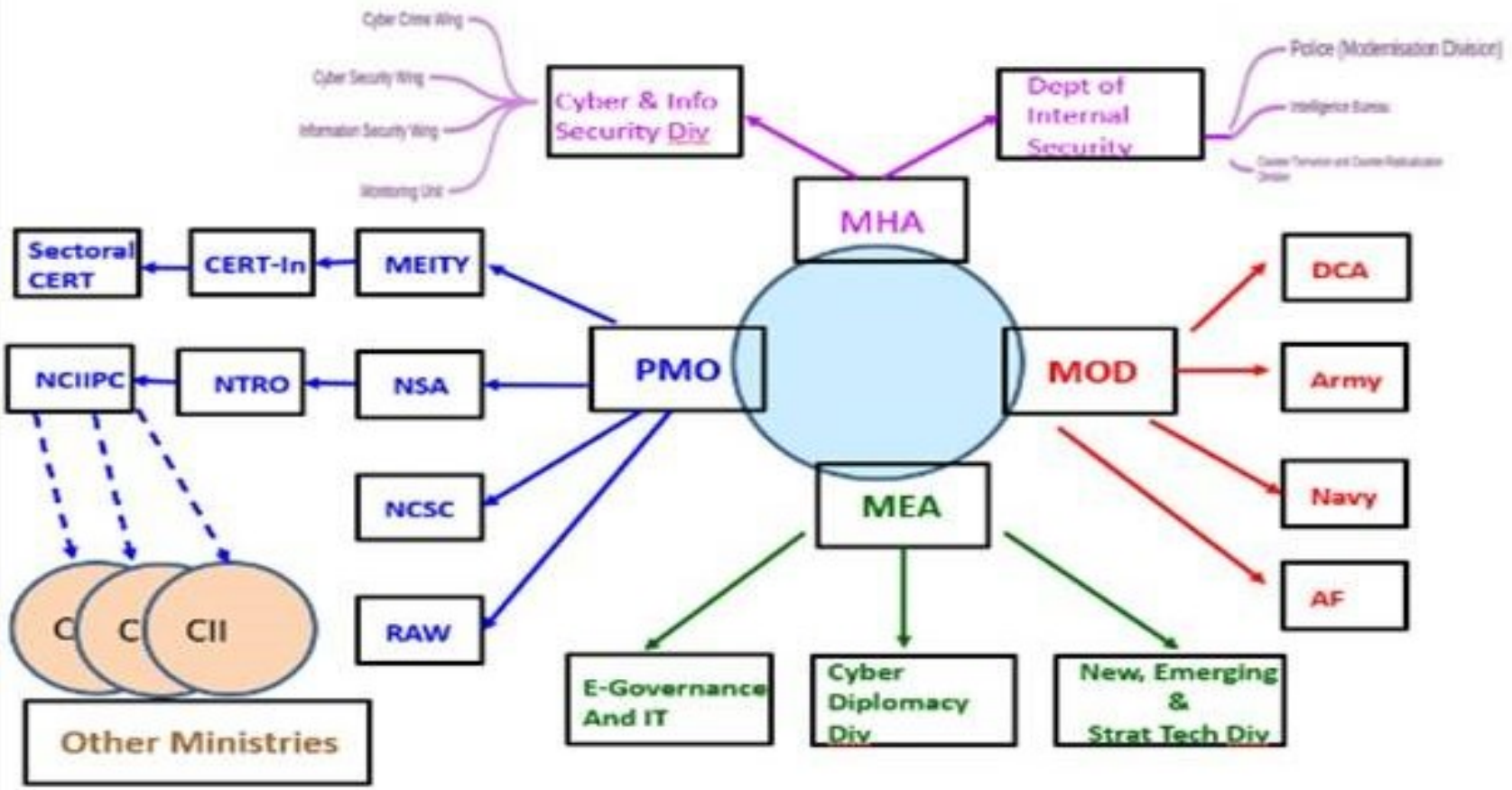
IMO-The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

PM MODI'S MARITIME MANTRA

OUT COME DOCUMENTS OF ALMOST ALL OF **PM MODI'S TALKS** WITH FOREIGN LEADERS WHETHER IN INDIA OR ABROAD INVARIABLY HAVE FOLLOWING COMPONENTS :

- MARITIME SECURITY & COOPERATION
- MARITIME INFORMATION AND INTELLIGENCE SHARING
- CYBER SECURITY
- COUNTER -TERRORISM

The Architecture of Cybersecurity Institutions in the Government of India



CONCLUSION

MARITIME CYBER THREAT WILL ONLY GROW WITH DIGITIATION

BIGGEST ASYMMETRIC THREAT AT SEA –

-WITH OUT A SHOT BEING FIRED

- WITH OUT CROSSING BORDERS

CAT & MOUSE GAME

HYBRID THREAT

CYBER THREAT- MARITIME

INFORMATION WARFARE

ELECTRONIC WARFARE

NETWORK CENTRIC WARFARE

PROXY WAR

DRONE WARFARE

PSY-OPS

SOCIAL MEDIA CAMPAIGN

THANK YOU