CyberSecPro

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Funded by the European Union

Critical Infrastructure Security for Maritime

Course

CSP008_C_M

PRESENTATION BY: BRUNO BENDER

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

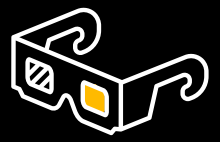
Risks of Maritime Critical Infrastructure

01. Identify Cybersecurity Risk for Maritime critical Infrastructure
02. Annual course as part of Maritime workshops – presential - Toulon)
03. Critical Infrastructure, OES, Maritime stakeholders
04. National specificities - NIS directive
05. Importance of data (EUCI, Sensitive,….)
06. Risk assessment and mitigation (e.g. Cryptography)
07. C2B Consulting

115 rue du maréchal Foch –F83.200 LE REVEST – France

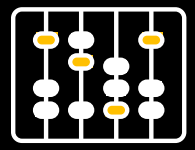
Goals: This module, designed for Maritime stakeholders aims at identifying risks for Critical infrastructure to improve their resilience

WHO



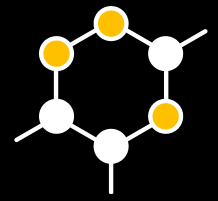
Mqritime Critical infrastructure and OES as identified in the NIS directive

WHAT



Foundational of cybersecurity Risk Management in the maritime domain

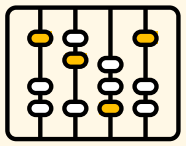
WHY



Equipping participants with the knowledge and skills necessary to manage Cybersecurity risks

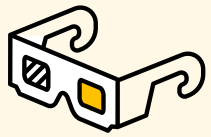
CSP Training Logistic: CSP003_ RISKS OF MARITIME CRITICAL INFRASTRUCTURE

WHEN



Time schedule: Autumn 2024 – Automn 2025

WHERE

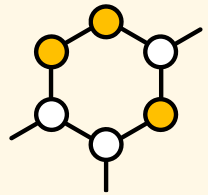


ONSITE-Location

Toulon (France)

NMIOTC (Greece)

HOW



- Theory
- On-hands training

WHO

Profile of Training Participants

- Managers and Leaders
- Working-life professionals
- SMEs and Public Sector Employees
- ~~Cybersecurity practitioners and enthusiasts~~
- ~~Maritime CIS developers~~

WHO

Profile of Trainer

- Bruno BENDER
- C2B CONSULTING
- Former Navy Officer / CIS specialist
- Information Security officer
  - NATO
  - Nationally
  - EU
- Since 2017 Cybersecurity expert & founder of C2B
- SME specialized in Maritime security / Cybersecurity to support
  - Critical Infrastructures
  - Operators of essential services
  - Maritime companies & harbors
  - Public administrations operating at sea

WHAT

Training Topics

- What is the definition of a critical infrastrucure
- User communities
- Technical architectures / INFRASTRUCTURES
  - Administrations
  - Technical description
- Risks
- Security Architecture Design
- Security Implementation
- Mitigations

WHY

Learning Outcomes

- Demonstrate ethical and professional conduct in all aspects of information and cybersecurity management.
- Comprehend and articulate the key concepts and principles of information and cybersecurity.
- Understand the evolving cyber threat landscape and the diverse range of cyberattacks.
- Identifies the cybersecurity threats, vulnerabilities, and risks to an organisation.
- Recognises the human factor's role in cybersecurity breaches and risk mitigation strategies.
- Ability to help and select appropriate security controls to protect against identified cybersecurity threats and risks.

Topic-1:
Cybersecurity Risks in the Maritime domains

We will cover these skills

- Introduction to information security: This section will introduce the concept of information security and its importance to organisations. It will also discuss the different types of information assets that need to be protected, as well as the different threats and vulnerabilities that these assets face.
- Introduction to cybersecurity: This section will focus on the specific threats and vulnerabilities that exist in the cyber domain. It will also discuss the different types of cyber attacks that can be launched, as well as the different ways to mitigate these attacks.
- The CIA triad: This section will discuss the three pillars of information security: confidentiality, integrity, and availability. It will explain what each pillar means and why it is important.
- Other security models: This section will discuss other security models that can be used to protect information assets. These models include the NIST Cybersecurity Framework, the ISO/IEC 27001 standard, and the COBIT framework.

Topic-2:
Threats and vulnerabilities

We will cover these skills

- 1. AIS: What is a critical infrastructure – Legal use and specificities
- 2. Description of a CI framework including hardware, software, and networks.
- 3. Ways Critical infrastructures are threatened
- Ataackers
- Mitigations
- 4. Reslience plans and actions
- Other

Topic-3:
Use cases

We will cover these skills

- 1. National plans
- 2. Local Mitigations
- 3. Education / Training
- 4. Investigations and lessons learned from the past
- 5. Threats and Risks
- 5. Mitigations
  - - Technical
  - - Organisational
  - - Insurance

CyberSecPro

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Funded by the European Union

Critical Infrastructure Security for Maritime

Course

CSP0008_C_M

PRESENTATION BY: BRUNO BENDER

Critical Infrastructure Security for Maritime

Topic 1 – General data

- Maritime / Cyber framework
- Cybersecurity and technology

Cybersecurity – not only technology

Services

Protection Services

EU CERT-M

Technical

End/End monitoring

Adaptive maintenance

Organisational

Maritime cyber Governance

Semantics

Assess & manage Risks, Rise incidents, Share analysis

ETSI GS ISI 00X: "Information Security Indicators (ISI)…"

Legal

Commercial Sensitive data, Personnel data, Positions,

Maritime Cybersecurity Risk

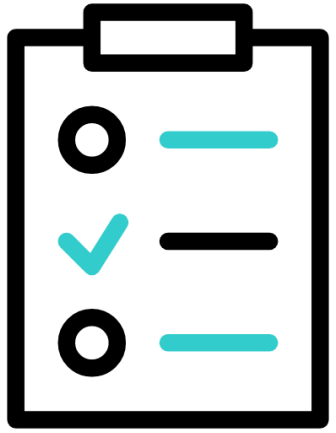
Objective

Course C2B_CSP008 aims at describing the cybersecurity risks in the maritime environment and to identify its specificities.

A focus is done on the AIS standards and specificities as well as on international regulation. Common vulnerabilities of AIS/GNSS systems and applications are detailed.

Methods and examples of hacking and spoofing of these systems are demonstrated during the course.

Risk analysis, security plans, policies and processes, regulatory framework and security standards continuity and recovery measures are presented.



Maritime Cybersecurity Risk

Cybersecurity threat to the Maritime

- Worldwide panorama
- Attacks / Incidents
- Evolutions

Risk in the Maritime domain / Mitigations

What systems

EU Coastguard Cybersecurity

Achievements - The continuation of the current efforts

Build on the initiative of the ECGFF workshops on "Cyber Attack Prevention in the Maritime Domain" initiated by the German presidency, and implementing a "EU Coastguard Cybersecurity Working Group".

Need to furthermore develop common approach of cyber-security for the coastguard community. For that, the legal, organizational and technical understanding shall be further developed together improving the cross-sectoral and cross-border cooperation, elaborating guidelines and best management practice to this end.

Animation of the coastguard cybersecurity community and implementation of an information sharing platform dedicated to cybersecurity and hosted by EMSA.

Consensual validation of the "EU Coastguard Cybersecurity Working Group" terms of reference addressed to the EU Commission (DG MARE).

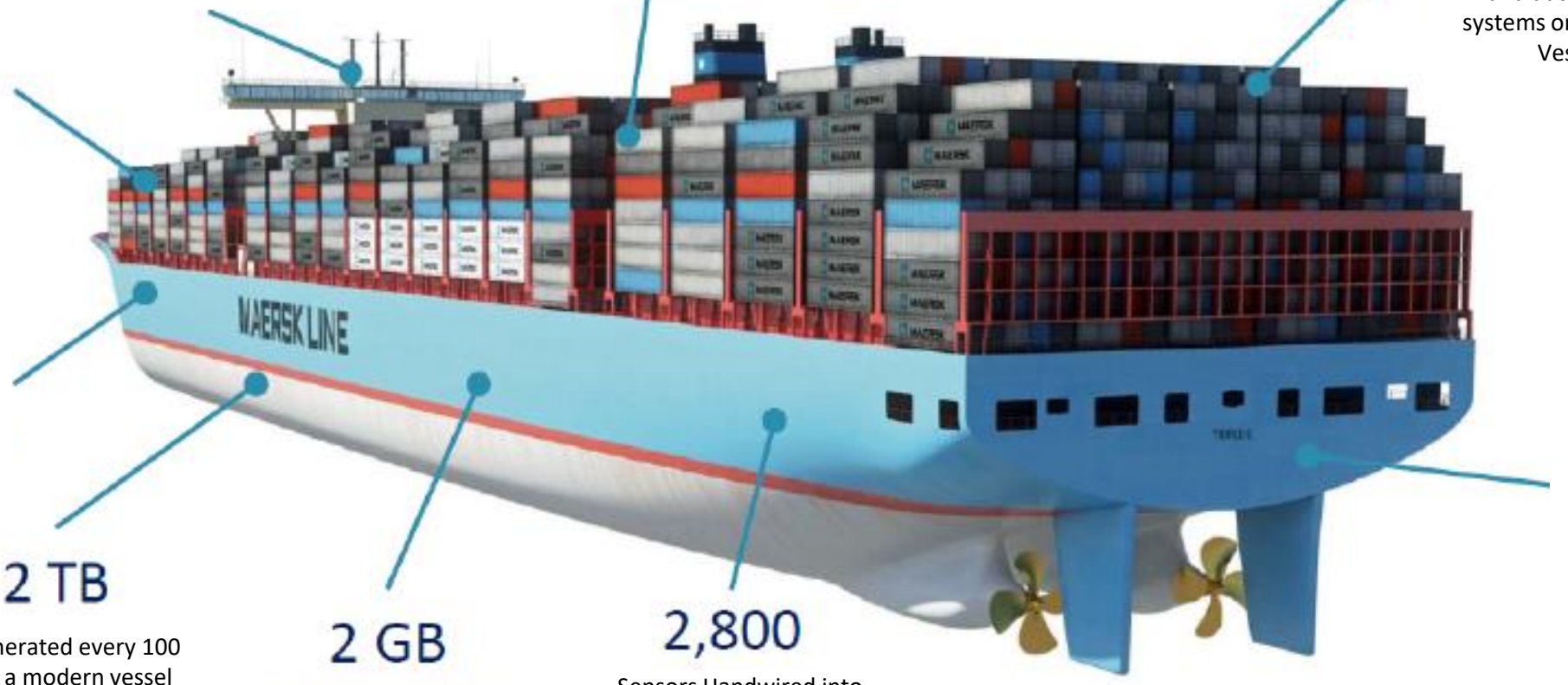
Support for further improvements on information-sharing processes for timely information exchange on cyber-attacks and incidents targeting the maritime community.

Continuation during the Croatian Chairmanship of the ECGFF (2019-2020).

Maritime Cybersecurity

- **Cybersecurity threat to the maritime**
- Maritime Data
- Worldwide panorama
- Attacks / Incidents
- Risks

The Risk of data in the Maritime



30 TB
Data Transmitted by MAERSK Line fleet over satellite every month

7,000
Channels monitored on the Triple E vessels for Situational Awareness and alarms

450,000
Meters of electrical cables for the electrical and automation systems on a Triple E Vessel

5,000
Data Tags on a modern Vessel

0.05
Seconds between each motion measurement on a ship

2 TB
Data generated every 100 days by a modern vessel

2 GB
Data Stored every da from the main contro system on a Triple E vessel

2,800
Sensors Handwired into the triple E vessels Main control system

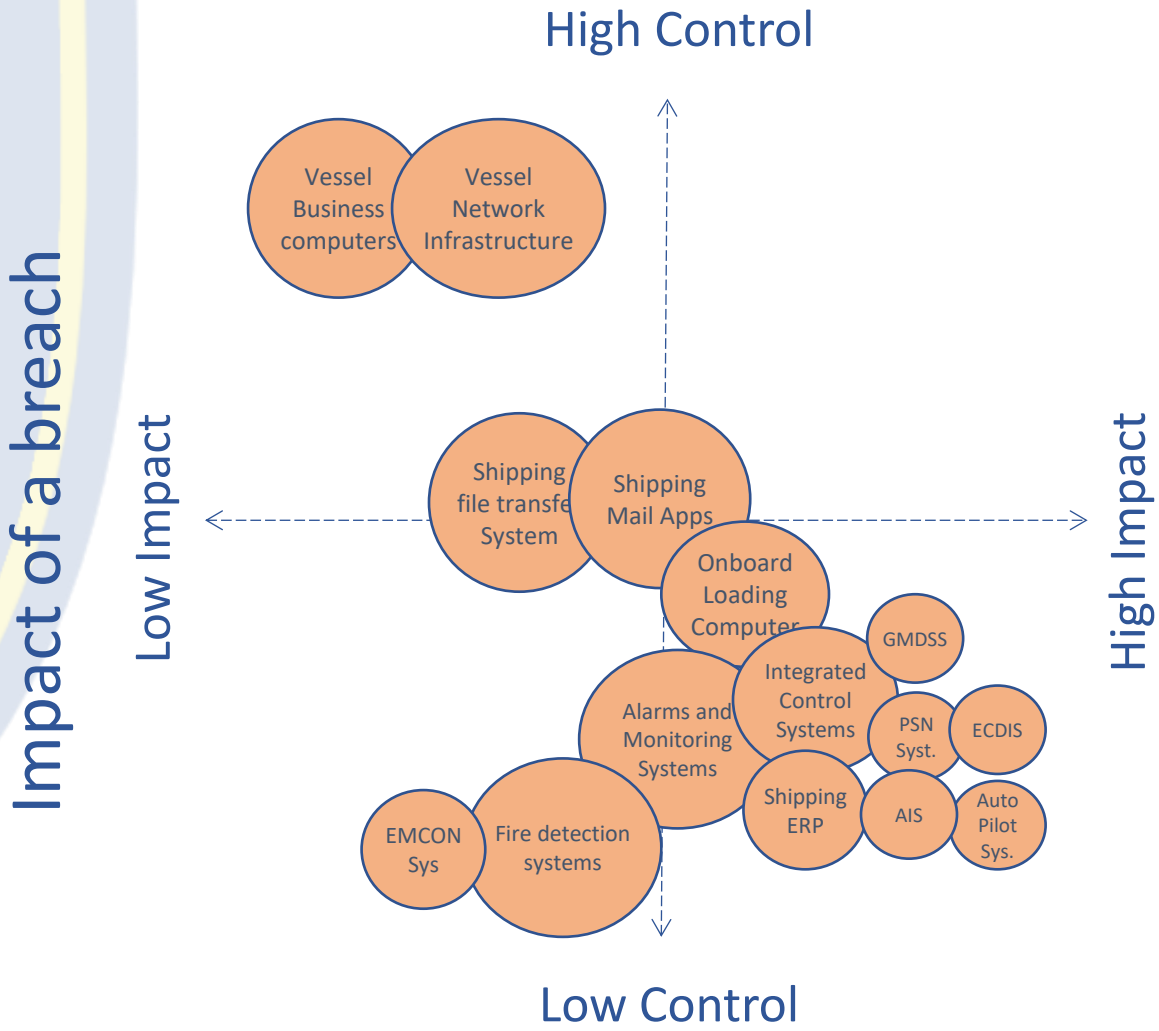
200
Sensors in a modern main engine room to monitor temperature, pressure, flows and operations

MAERSK

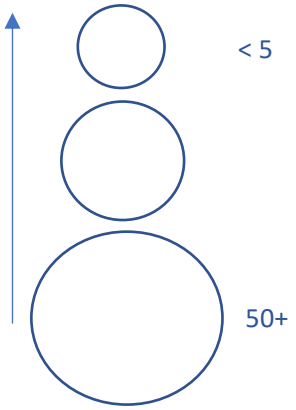
Critical Infrastructure - Shipping authorities

Control on security / Impacts of incidents

Control of Security by Shipowner



Nb users / impacted systems



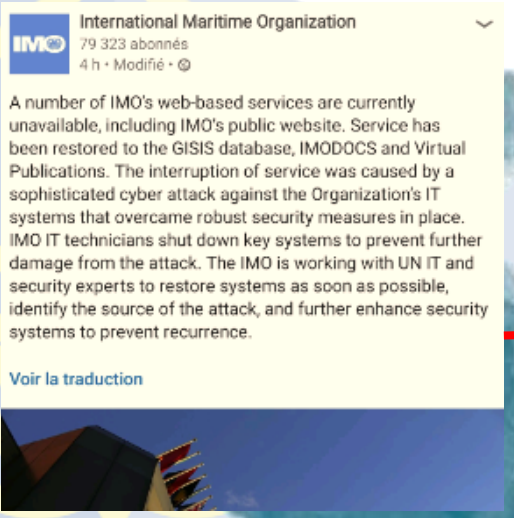
Critical Infrastructure Security for Maritime

Topic 2 – Threats and vulnerabilities

- Cartography of Maritime systems
- Threats – Worldwide
- Observed Events Incidents

Threats - Major Attacks 2020 - 2023

Worldwide



Mar 2020 – Switzerland (MSC)

Dec 2019 – Elbe (Spoofing AIS)

Apr 2020 – Ormuz Bandar Abbas

Sept 2020 – Int (CMA-CGM)

May 2020 – California (Spoofing AIS)

Sept 2020 – Int (GEFCO)

Mars 2020 – Marseille / FOS – Regional Attack

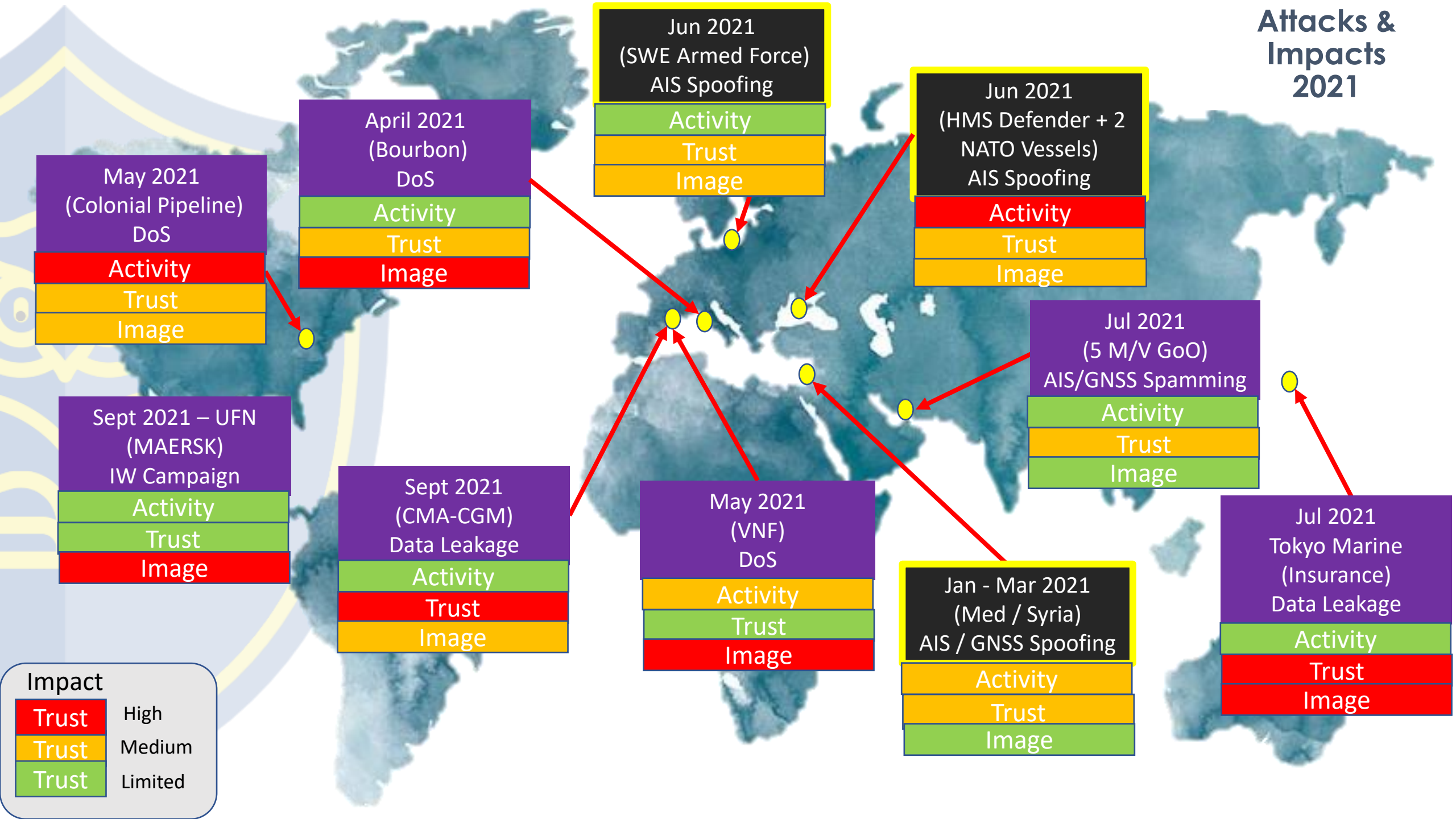
2020 – Mediterranée (Brouillage GPS)

Jan 2020 –China (Spoofing AIS)

Attacks / incidents (2020 – 22)

Entity	Date	Impact	Analysis
Port of Bandar Abbas	2020	Inability to implement loading and unloading terminals	Deliberate **targeting of a "non-critical" port by a country** in a pre-emptive attack resulting in an immediate response
MSC	2020	Inoperable services (>12 h) Web page and customer interface inaccessible for several days in some areas	**Locally hosted services** have allowed the operator to continue to operate in certain regions
MED EUROPE TERMINAL	2020	Blocked Internet services that have impacted the web portal and messaging.	The maritime operator was the **collateral victim** of an attack on the Southern Region during the containment of the
GNSS/AIS	2018 - 2020	Saturation of AIS receivers (observed in the Mediterranean in 2019, in China in the USA in 2020) Permanent GPS jamming in Eastern Med, China & Black Sea	The interference or Spoofing (saturation) of GNSS /AISrepresents a real **danger to navigation**. Observable in their crudest forms attacks on GNSS/AIS systems can eventually **distort all maritime data**.
CARNIVAL	2020	Loss of customer and employee data. Loss of activity on the cruise (bookings)	Classic ransomware attack that encrypted part of CIS systems and data and blocked the activity for several hours.
CMA / CGM	2020	Data and services incassesible due tiocryptolocker Loss of customers	The attack was remediated in more than 2 weeks by specialists **not familiar with the companys CIS**. The communication has to focus on the operators priorities.
BENETEAU	2021	Attack on systems and loss of Data	BENETEAU has been attacked a first time in 2018 and has lost data (customer lists) a second time in less than 3 years
BOURBON	2021	Attack on main exploitation System	Problems to manage the crew changes and the daily activity and reports for ships
GAZOCEAN	2021	President Rip-Off	Financial Los
VNF	2021	Attack on Main information System	Management systme blocked for several days
Port of Abidjan	2021	Ransomware MATRIX	Limited impact maritime trafic reported after coordinated reaction
DNV-GL	2020	Spying for a State - Data Theft Image of the skipped society	Class societies are often exosed to this kind of risk due to the information they are accessing

Attacks & Impacts 2021



CMA / CGM Attack 2020

Édition du jeudi 31 octobre 2024
Feuilleter l'édition

LA LETTRE

La Matinale | Se connecter | S'abonner

Menu | À la Une | Action publique | Entreprises | Médias | Paris-Bruxelles | Enquêtes | Entourages | Mouvements | Feuilletons

L'enquête sur la cyberattaque de CMA CGM avance à grands pas

Si la plupart des enquêtes sur les rançongiciels échouent à identifier les hackers, les cybergendarmes ont arrêté en Ukraine des suspects dans l'attaque qui a ciblé le transporteur maritime CMA CGM en 2020. L'enquête en cours confirme les premières pistes sur le gang Ragnar Locker. [...]

Publié le 07/12/2021 à 6h30 • Lecture 2 minutes

Créez une veille sur les mots-clés cités dans cet article

Agence Nationale de la Securite des Systemes d'Information

CMA CGM

The investigation into the CMA CGM cyberattack is making rapid progress If most ransomware investigations fail to identify the hackers, cyber police have arrested suspects in Ukraine in the attack which targeted the maritime carrier CMA CGM in 2020. The ongoing investigation confirms the first leads on the Ragnar gang Locker. [...]

Use case - ransomware

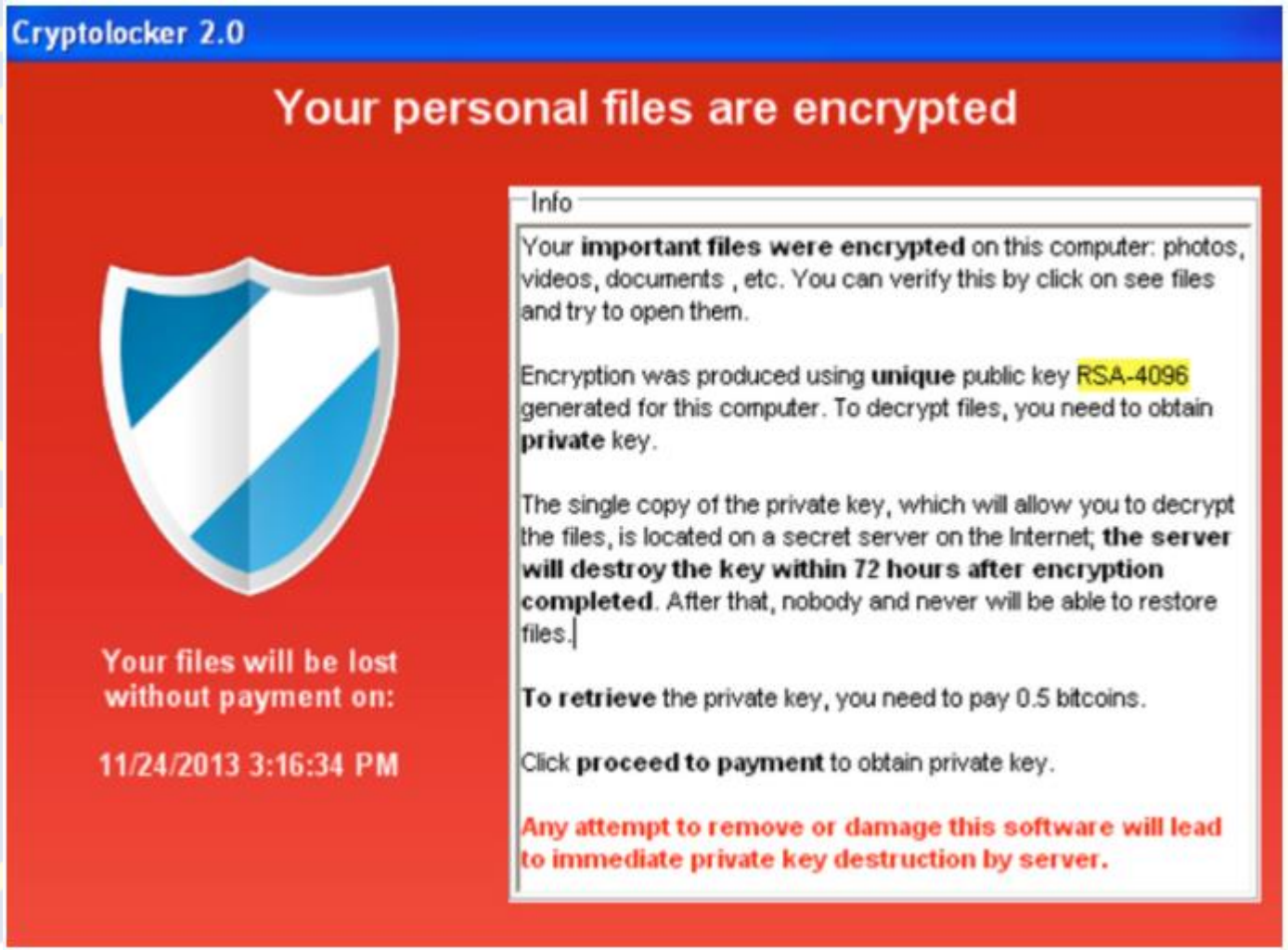
- **What is a “ransomware”**
  - Malware which threaten damages unless a ransom is paid

- **Types**
  - *Screen locker*
  - *File cryptor*
  - *DDOS*
  - *Combined*

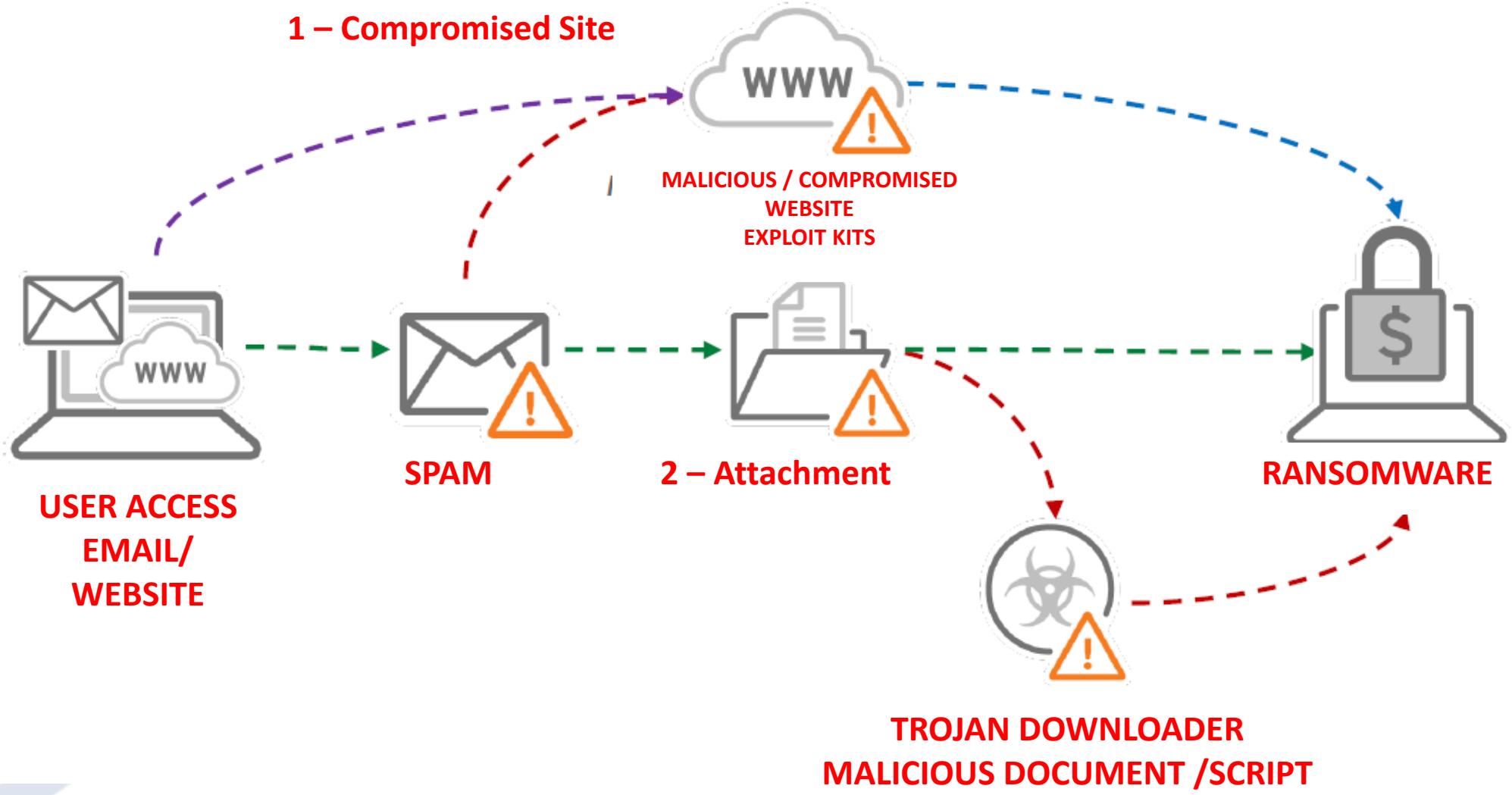
Source: Trend Micro

INTRO – Screen locker

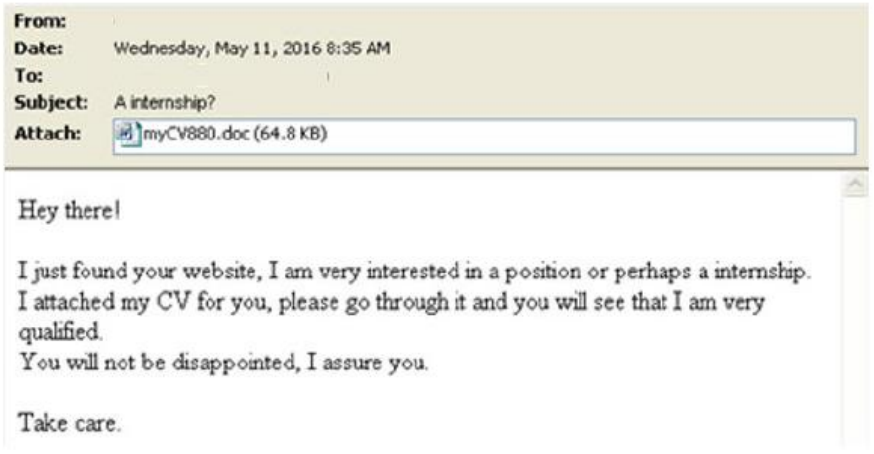
INTRO – File cryptor

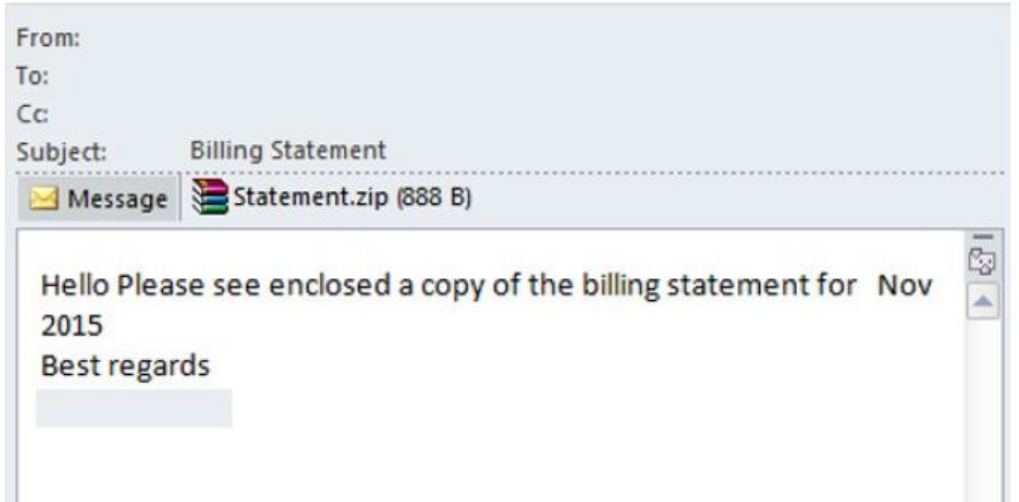


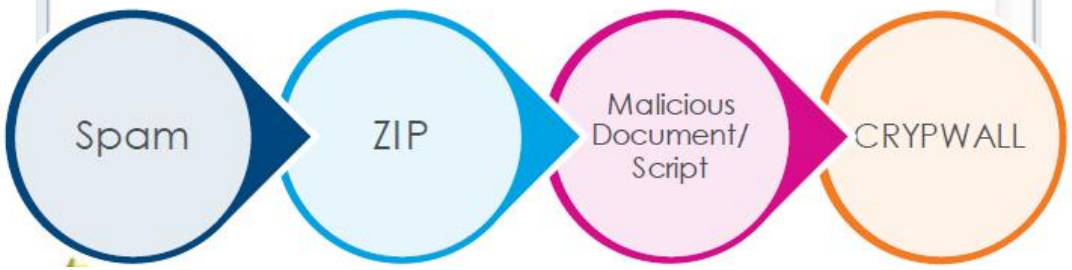
"COMMON" ARRIVAL VECTOR



"COMMON" ARRIVAL VECTOR

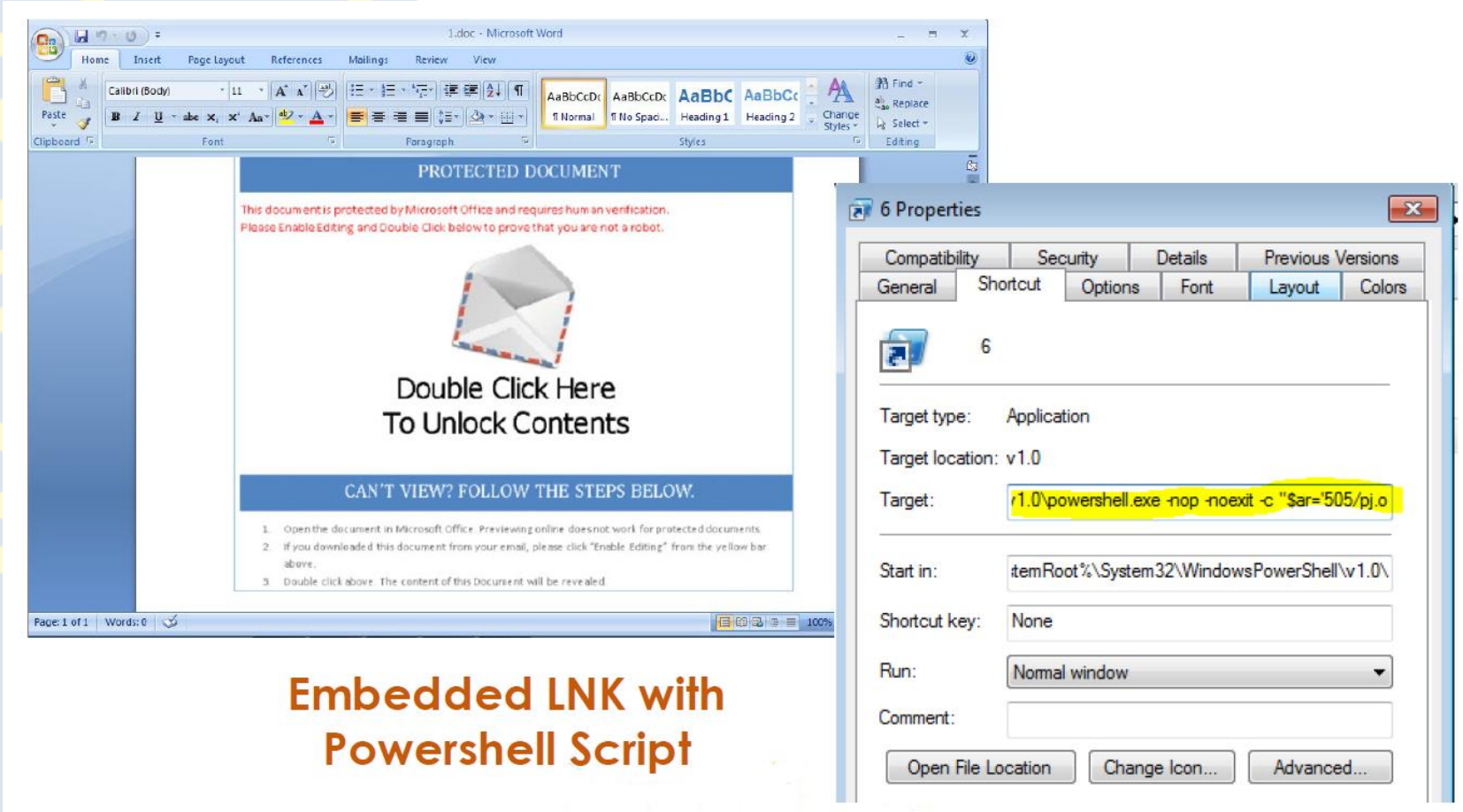






Source: Trend Micro

"COMMON" ARRIVAL VECTOR



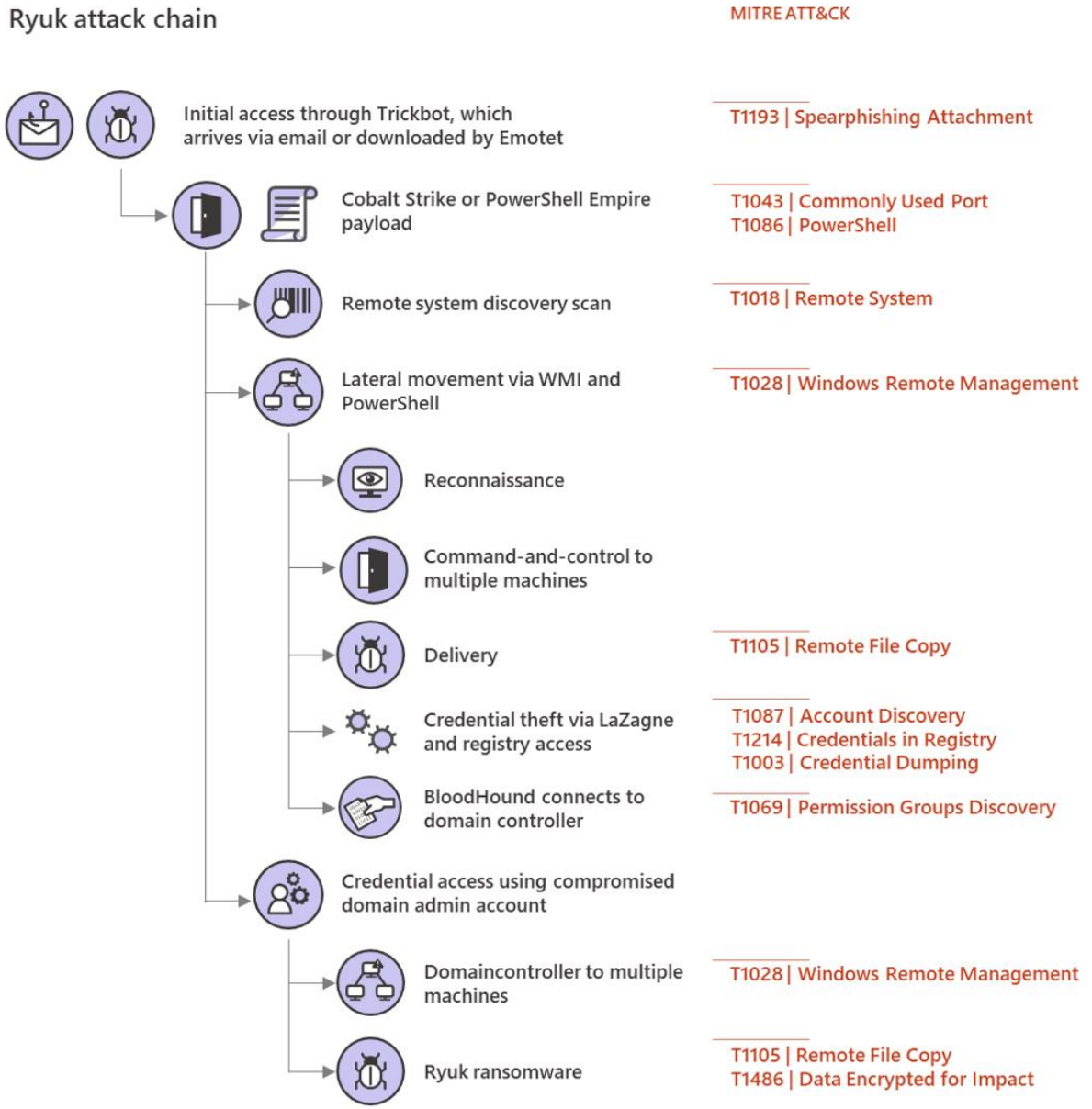
Source: Trend Micro

INTRO – HISTORY

- 1989 – "PC CYBORG"
  - blocked PC for "expired license"
  - distributed @ WHO AIDS conference (floppy disk)
  - disk file encryption
- 2005-2006 – first wave of "modern" ransomware (in Russia)
- 2011 – SMS ransomware (dial a premium SMS number)
- 2012 – Fake police-based "Screen Locker" ransomware
- 2013 – Cryptolocker (strong encryption, use of TOR)
- 2014 – File cryptor "frenzy": CryptoWall, CTB-Locker, Locky, TeslaCrypt …
- 2017 – WannaCry (with "worm" capabilities)
- 2018 – NotPetya (eraser)
  - hit "Maersk" danish maritime company (10 days off!)
- 2019 – Maze (double extortion)
- 2021 – Triple extortion (adding DDOS threat)

NEW TRENDs

- **Human-Operated Ransomware**
  - customized infection vectors (reconnaissance)
  - (high-value) target discovery
  - Privilege escalation – Lateral Movement
  - APT-like TTP



Source: Microsoft

"COMMON" TRENDS

- **Initial Access Broker (IAB)**
  - Find a way to gain foothold in "random" organizations networks
  - Sell the network access (usually via dark web, 500-10.000$)
- **RaaS** – Ransomware As a Service
  - malware can be brought
  - Malware remote usage platform can be brought
    - Configuration: ransom fee, payment note, victims…
  - the platform may already provide victim access
    - e.g. Emotet (generic downloader)

Topic 2 - Threats

Maritime Sector

- Identified sources
- Use cases

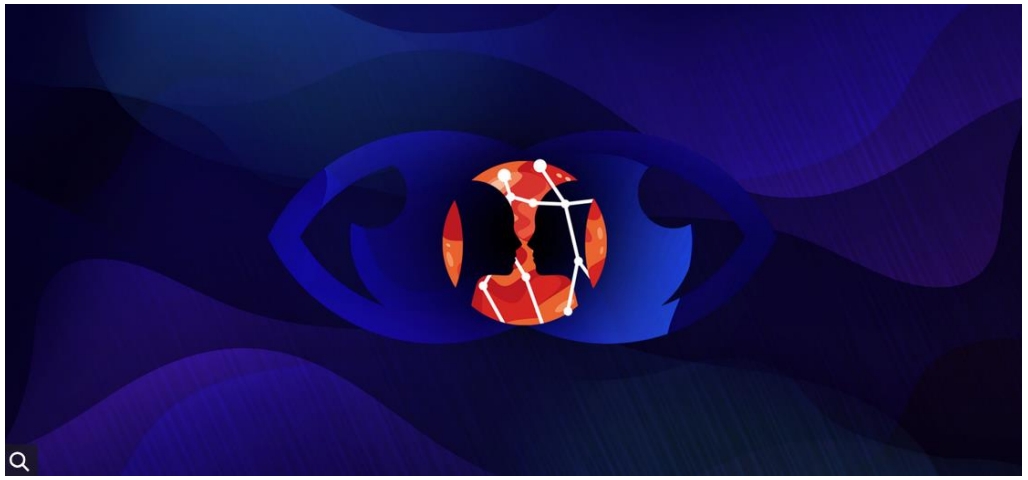
HARBOURS & MARITIME STAKEHOLDERS

Intelligence sources (Companies)

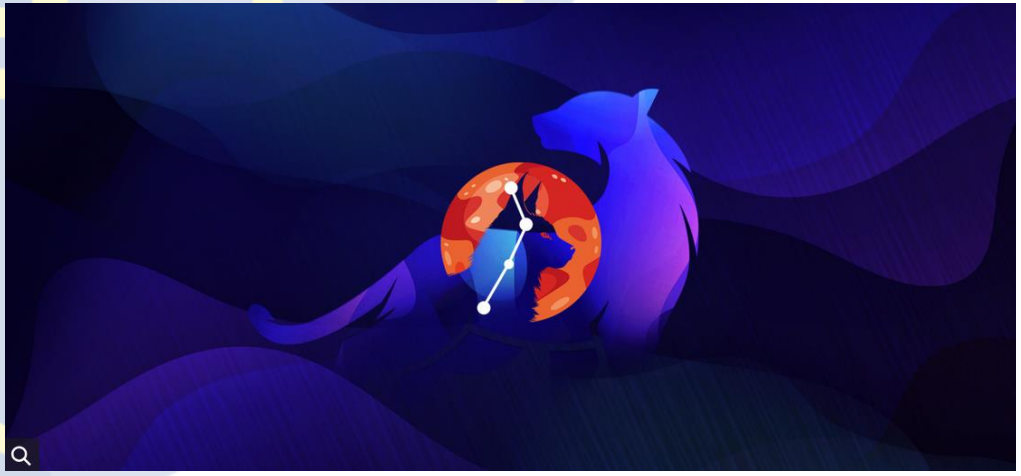
Threat Actor Groups Tracked by Palo Alto Networks Unit 42

RaaS platform : https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/

Draco PAKISTAN



Gemini INDIA

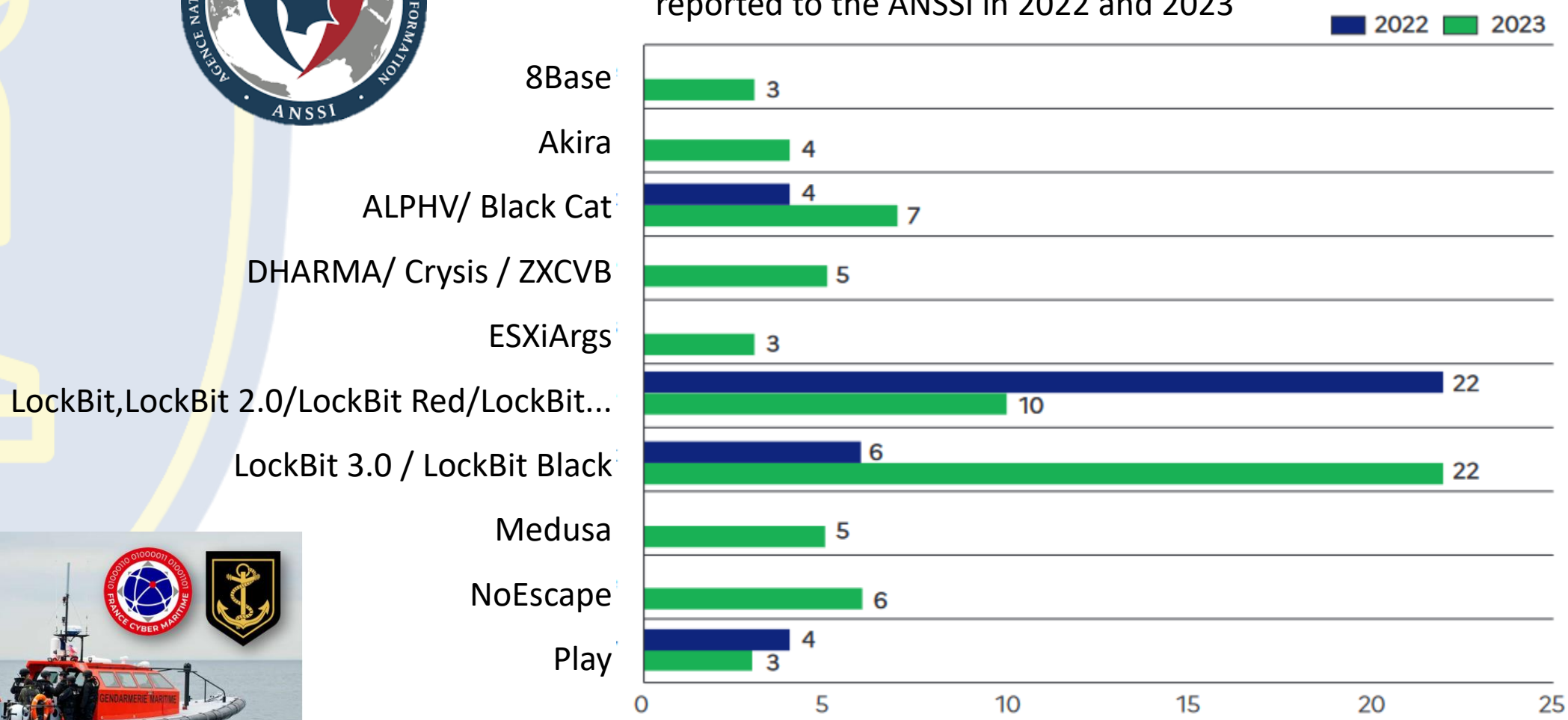


Lynx BELARUS

Issue : The legal location of Rogue actors

RaaS: RANSOM As a Service

Intelligence sources (National Agencies)



RANSOMWARE in the maritime domain

- **Trends**
  - increasing digitalization
  - natural shift from locally conducted operation to remote
  - COVID-19 remote boost
- **Ransomware attacks – peculiar aspects?**
  - same attackers, same TTPs
  - interesting target: supports 90% of worldwide trade!
    - potential war target
  - complex and integrated IT ecosystems (also with Operation Technology – OT)
    - supply chain increased risks: the “entrance point” may be a partner company!
    - many attack vectors available for the attackers
  - shipment are key point in the logistic supply chain
    - can be used an intermediate step to other target (supply chain attack)

RANSOMWARE in the maritime domain

Ransomware attack on US maritime facility confirmed

Story By: Rob O'Dwyer | January 8, 2020 | Blockchain and Cyber Security

The US Coast Guard (USCG) has issued a marine safety bulletin confirming a recent ransomware attack at a Maritime Transportation Security Act (MTSA) regulated facility, which locked users out of access to critical files and saw the infection move beyond the local facility and into wider corporate networks.

Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data

Swire Pacific Offshore notified authorites of a cyber attack on its systems (Swire file photo)

PUBLISHED NOV 26, 2021 12:05 PM BY **THE MARITIME EXECUTIVE**

Image: Dimitry Anikin

With today's news that French shipping giant CMA CGM has been hit by a ransomware attack, this now means that all of the four biggest maritime shipping companies in the world have been hit by cyber-attacks in the past four years, since 2017.

Previous incidents included:

1. APM-Maersk - taken down for weeks by the NotPetya ransomware/wiper in 2017.
2. Mediterranean Shipping Company - hit in April 2020 by an unnamed malware strain that brought down its data center for days.
3. COSCO - brought down for weeks by ransomware in July 2018.

Solutions

- **Just implements IT Security best practices**
- **Main mitigation topics**
  - **strong authentication** (especially for internet-facing portals and VPNs)
    - or **zero-trust approach**, in a perimeter-less approach
  - **least privilege principle** (especially with user privileges)
  - **system\network segregation (physical\logical)**
  - **Business continuity** procedures
    - **backup** (hot and cold)
  - Continuous **vulnerability assessment** and **patching**
  - **Security Operation Center** monitoring
  - **Hardening (**network protocols, host firewall, software configuration, OS security, …)

Use case – AIS / GNSS

Main concern for Maritime Agencies – AIS / GNSS Spoofing / Jamming

EUROPEAN COAST GUARD FUNCTIONS FORUM

June 2021 – ECGFF cybersecurity working group Note on cybersecurity incident

N° 1/2021

UNCLASS – For Official Use Only

The AIS positions of two NATO ships were spoofed near the Russian naval base in the Black Sea.

The analysis of the present note shows an example of spoofed AIS information that could represent a threat on activities conducted by vessels conducting maritime operations. It confirms the leaks of AIS used by vessels operated by public administration an raises the need to develop our work initiated within this group.

Tracking data from two NATO warships were falsified off the coast of a Russian-controlled naval base in the Black Sea while the ships were at harbour visit 180 miles away.

The British Royal Navy's HMS Defender, a Daring Type-45-class destroyer, and the Royal Netherlands Navy's HNLMS Evertsen, a De Zeven Provincien-class frigate, at Odessa, Ukraine, on 18 June. The group was marked by Russian warships during their transit through the Black Sea, as evidenced by U.S. Navy photos dated June 17.

According to the AIS, the ships left Odessa just before midnight on 18 June. Analysis of the data shows that they would have sailed directly to Sevastopol, approaching within 2Nq of the port that houses the Russian Black Sea fleet.

The two warships, however, did never leave Odessa. The webcam streams (see USNI slide) show that they have not left Odessa, however. The webcams are streamed live on YouTube by Odessa Online. Screenshots archived by third-party weather sites like Windy.com show the two warships present in Odessa during the night.

The positioning of two NATO warships at the entrance to a major Russian naval base is widely perceived as provocative action.

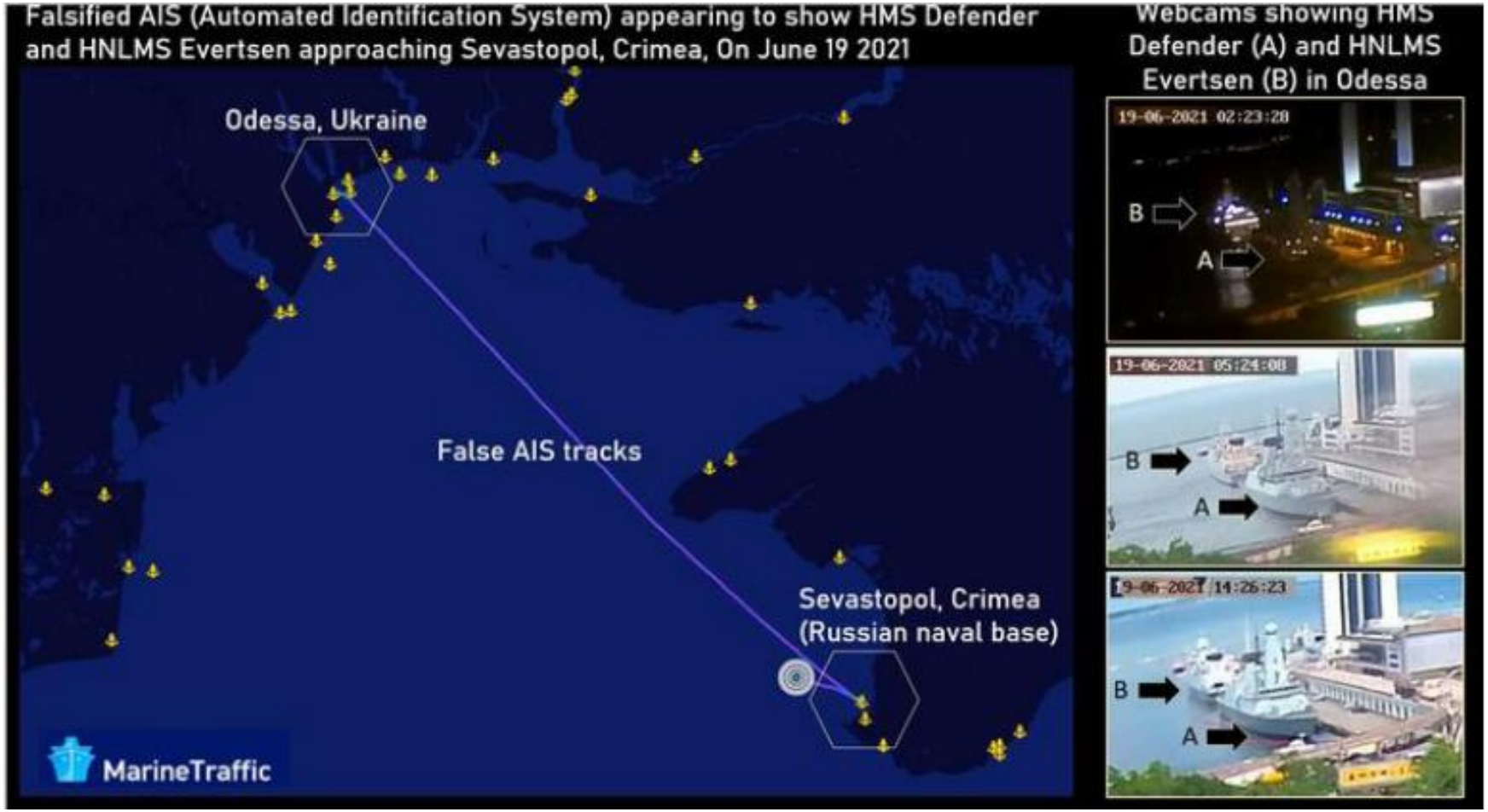
Although the reasons for spoofing are not clear, this decision raises questions about the effectiveness of open source intelligence data, such as AIS, which is becoming increasingly common in the defense and by journalists.

There is irrefutable evidence that the AIS tracks were spoofed by a third party.

NATO officials did not immediately respond to requests for comment and the traks identified on AIS providers (MarineTraffic.com in the present case) were confirmed as false by the Dutch news site Marineschepen.nl.

AIS positions were probably sent to MarineTraffic.com via the Chornomorsk ground station near Odessa operated under Russian control. Other AIS operators have also reported the false

The AIS positions of two NATO ships were spoofed near the Russian naval base in the Black Sea.



Sources:

- EU CERT & M-CERT
- Member States
- Private companies

Threats to Critical infrastructure

Malware:
Malware whose spread is uncontrollable

Script kiddy (idle teenager or, more generally, solitary and opportunistic striker):
- Very low means (€<,100)
- Gambling (and possibly profit) as motivation

Opportunistic attack Malicious employee (grudge/greed):
- Low means (< €1,000)
- Main motivation: to harm one's employer, avoiding victims
- Discretion when possible
- Easy access to all elements of the vessel

Terrorist group:
- Moderate means (from €10,000 to €50,000)
- Search for human victims, material damage, high media visibility

Criminal enterprise:
- High resources (around one million euros)
- Profitability objective
- Low moral constraints
- Seeks discretion

State:
- Almost unlimited means
- Objectives of all types –
- Absence of moral constraints
- Necessary discretion

Threats on Systems

Ship spoofing – AIS message is broadcast giving details of a non-existent ship. Scenarios where this could be used include spoofing a ship of one nation into the territorial waters of a hostile nation, leading that nation to take countermeasures. Alternatively, multiple versions of the details of a real ship can be broadcast, placing it in many different locations simultaneously to obscure its true location (e.g. illegal fishing).

Aid-to-navigation spoofing – Fake aid-to-navigation, such as a buoy warning of hidden shoals, are broadcast in order to force a ship to change its course. This might be done to force a vessel into a region where it can be hijacked.

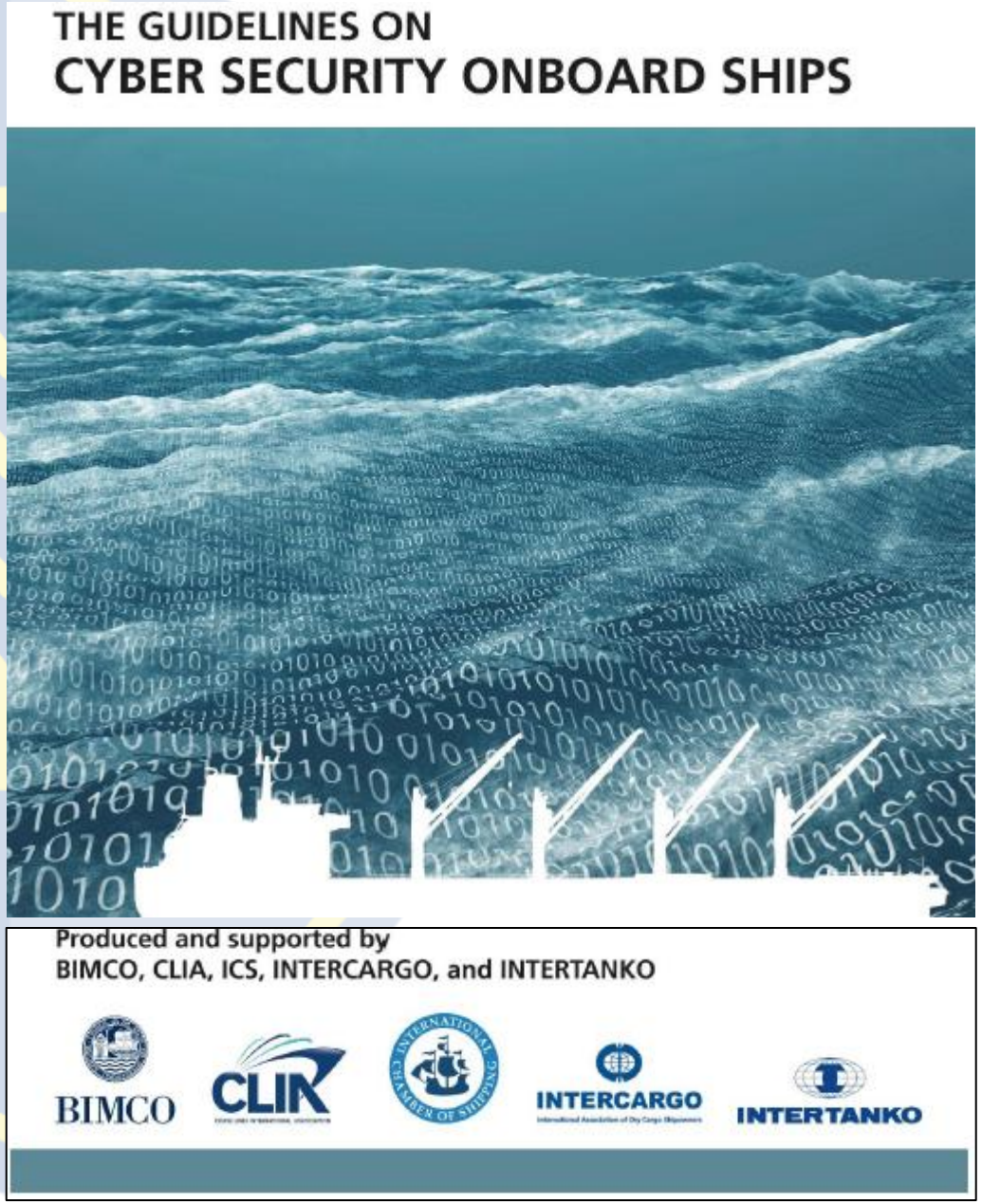
Collision spoofing – Collision avoidance is one of the primary uses of AIS. By providing spoofed details of a vessel on a collision course, an attacker can force a ship to change course to avoid the anticipated collision. This could, for example, be used to steer the ship into a real collision

AIS-SART spoofing – Search & rescue is another of the primary uses of AIS. This attack generates a spoofed SAR-T transponder signal, which gives details of a distress. As ships are legally obliged to assist, SART spoofing can be used as a decoy to lure vessels to a location where they can be attacked.

Weather forecast spoofing – AIS can be used to relay information about prevailing weather conditions between marine craft. A fake forecast, particularly one that predicts fine conditions when a storm is incoming, could be used to lead vessels into difficulties.

AIS hijacking – It is also possible to override signals being sent by vessels, by broadcasting a higher-power signal at the same time and frequency. The attacker can then change some details of the original message, for example to suggest that the vessel has a nuclear cargo in an area where such cargoes are illegal.

Shared responsibilities – Large community - Limited initiatives



- Flag countries
- Shipowners
- Ship management companies
- Harbours
- Connectors to economy (Regional, Transports)
- Maritime agents
- Insurance companies
- Certification agencies
- Shipbuilders
- COMMS operators
- System providers
- Security providers

Terms of Use

The advice and information given in the Guidelines on cybersecurity on board ships is intended purely as guidance **to be used at the user's own risk**. *No warranties or representations are given, nor is any duty of care or responsibility accepted by the Authors, their membership or employees of any person, firm, corporation or organization … for the accuracy of any information or advice given in the Guidelines or any omission from the Guidelines or for any consequence whatsoever resulting directly or indirectly from compliance with, adoption of or reliance on guidance contained in the Guidelines even if caused by a failure to exercise reasonable care on the part of any of the aforementioned parties.*

Threats / Impacts

Maritime Specificities

- Communities
- Similarity Maritime / Digital
- GNSS Dependance
- Information Sharing environment

Risks of Maritime Critical Infrastructure

Topic 3 – The importance of data

- EU Regulation
- Classified data / Sensitive data
- Processing of data

Maritime / Digital similarities

	Maritime	Digital
Dimension	80% of earth	Unlimited
Legal	Weak international regulation UNCLOS	Limited inernational Regulation GDPR
Economical	90 % of international Trade Stable	50 % of international transactions Permanent growth
Environment	Unpredictable: Sea state, Wind, Salt, Physical dangers	Unpredictable: Virtuality,
Threat	Illegal activities and handlings, Piracy, Terrorism	Global Scope of Cyberthreats Illegal activities focused on goods
Focus	Share information (IFC) Acting capacities = States	Prevent & Share information Coordinate action

Maritime & Digital : similarities

Similar worlds (same assessments – same consequences ???)

800 - 1260 T rubish

In 10 seconds….

225,000 GB data

- 500,000 posts Facebook,
- 57,000 tweets,
- 46,000 recherches Google
- 2 million de messages sur WhatsAp

Communication Plan

Adapted to the operators

Critical Infrastructure

ECI Directive 2008

Global Risk (security, espionnage, data, activity)

Attack could endanger a countries security

Sectoral monitoring
- Risk Analysis
- Vulnerabilities
- Directives

Cross sectorial Coordination

Operator of essential service

NIS Directive 2015

Risk of espionnage, data, activity

Attack could endanger the economic activity

Sectoral Risk Assessment

Warnings

Cross sectorial information

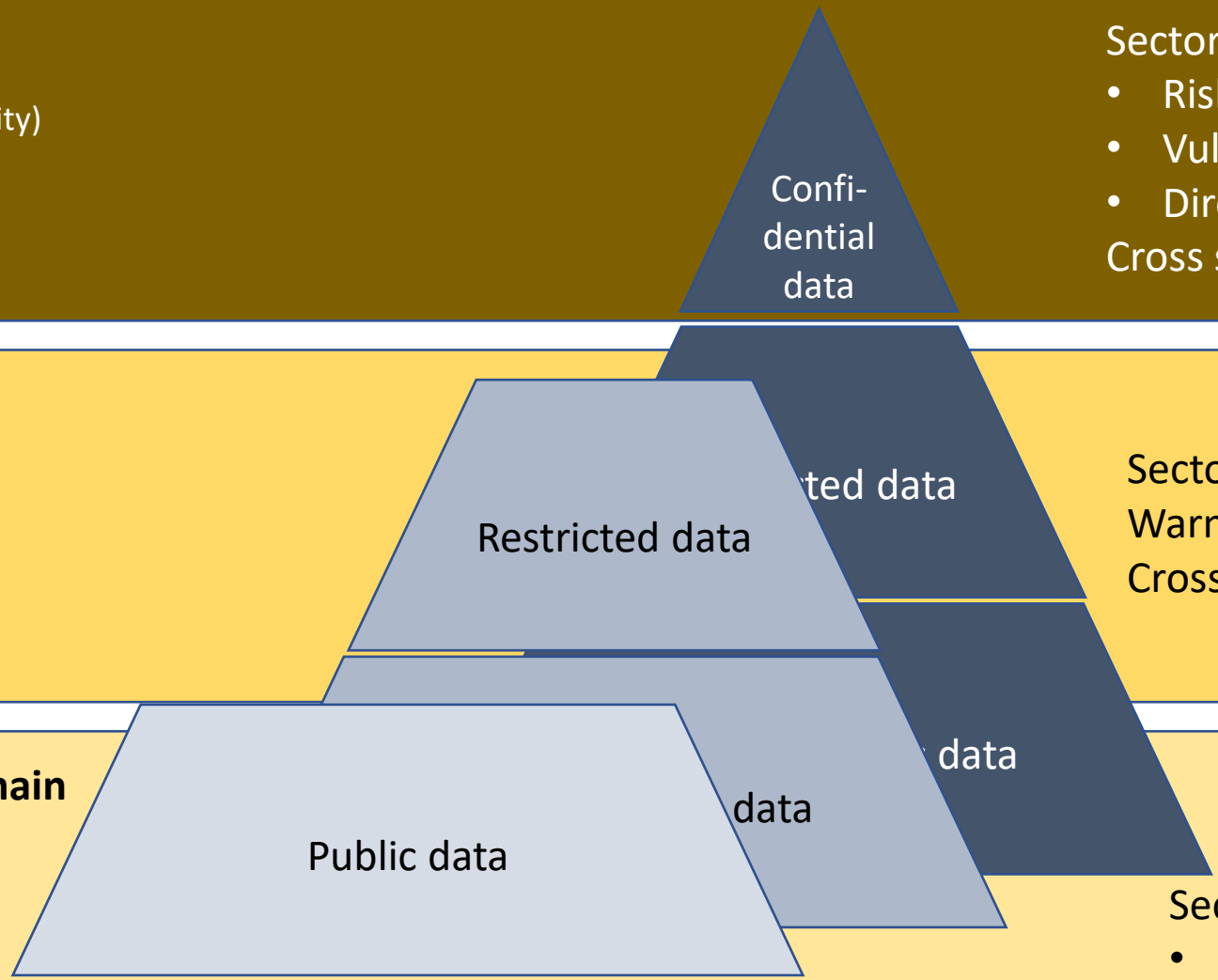
Common User of the Maritim domain

GDPR 2018

Risk for data

Attack could represent a threat

Sectoral Awareness
- Recommendations
- Prevention



Education & Training

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK: JOB PROFILES

- Chief Information Security Officer CISO
- Cyber incident Responder
- Cyber Legal, Policy And Compliance Officer
- Cyber threat Interlligence specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration tester

European Cybersecurity Skills Framework (ECSF)

https://digital-skills-jobs.europa.eu/en/cyber-skills-academy-knowledge-and-training

https://cybersecpro-project.eu/

Use Case
Critical Infrastructure
Maritime Harbor

HARBOURS & MARITIME STAKEHOLDERS

What objective for Attackers?

Information Assurance

Confidentiality	Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information	CRYPTO
Integrity	The property whereby an entity has not been modified in an unauthorized manner.	ACCESS CONTROL RIGHT
Availability	Being accessible and useable upon demand by an authorized entity.	BCP/BRP
Non-Repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.	D.SIGN
Authentication	Verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.	PASSWORD

Functionnal areas

(CYBERSECPRO Taxonomy)

Privacy and Data protection

Cybersecurity Risk management

Cybersecurity Threat management

Cyber Incident Response

Human aspect of cybersecurity

Penetration testing

Network and Communications security

Tools and Technology

Cybersecurity Management

Cybersecurity Policy, Process, Compliance

Maritime Framework – Legal (International)

IMO RESOLUTIONS

MSC.428(98) (16 June 2017) MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS:

an approved safety management system should take into account cyber risk management

Administrations should ensure that cyber risks are appropriately addressed in safety management systems 01 January 2021 (Survey ?)

Particular systems that should be considered:

- Bridge systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems
- Communication systems

Incident notification requirements

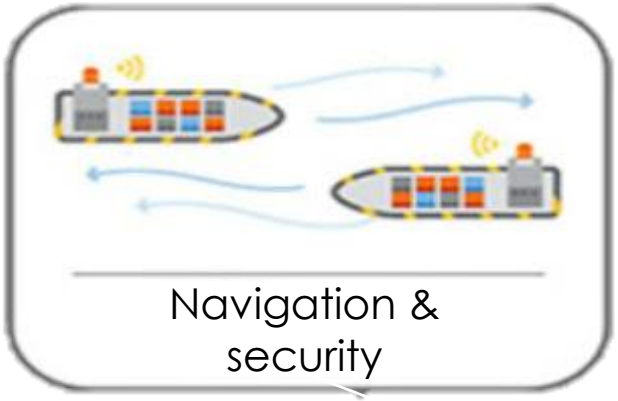
- Specific criteria/thresholds for incident notification

Maritime Framework – Legal (EU) - Reminder

	Reference	User	Net	SI	Who is concerned	Preventive measures	Ability to defend	Reconquest (Judicial)
C I (Nations : after- 2013) 	Directive 2005/65/EC National regulation	+++	++	++ +	Ports Cable Oil & gaz HAZMAT and their critical systems	EU has identified ports as critical infrastructure" Port = specified area of land and water, with boundaries defined by the MS, containing works and equipment designed to facilitate transport operations	Event Logging and Ability to Analyze Logs Probes to systems (State or qualified service provider. ANSSI permalink Crisis management	Retention of technical records for 6 months
OES (NIS – 2018 - 22) 	Dir (EU) 2016/1148 of the European Parliament and of the Council (6/07/16 - measures to ensure a level of security of systems and networks	0	+++	++	**OES** List provided by Nations (harbours, Maritime Companies)	List of essential services Political and technical governance. Network and IS protection. PM Decision Controls, Standards Cloud Provider Rules	Defense of networks and information systems; Use of hardware/software devices or IT services that have been certified for security. Reporting incidents to the National Security Agency.	Business resilience.
Data (GDPR-2018) 	EU Regulation 2016/679 - 27/04/16 data - physiical person protection Regulation	+++	0	++	Entity managing personal data (Ferry transport agent)	Protection of fundamental freedoms in the digital world (erasure and data portability.	Protected systems and networks at the level to prevent loss of control of personal information	Possible recourse to CERTs in the event of data loss/leakage.

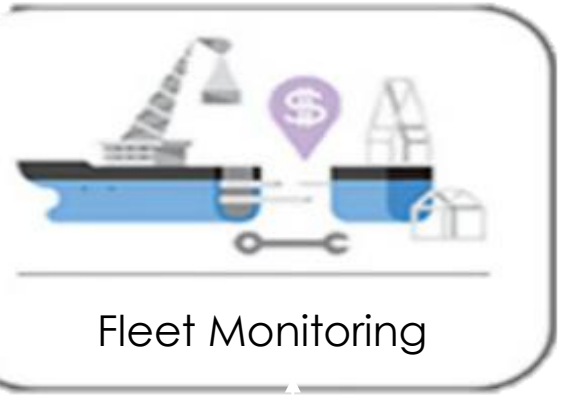
Port Control Systems (PCS)

Port Operations
What systems ?

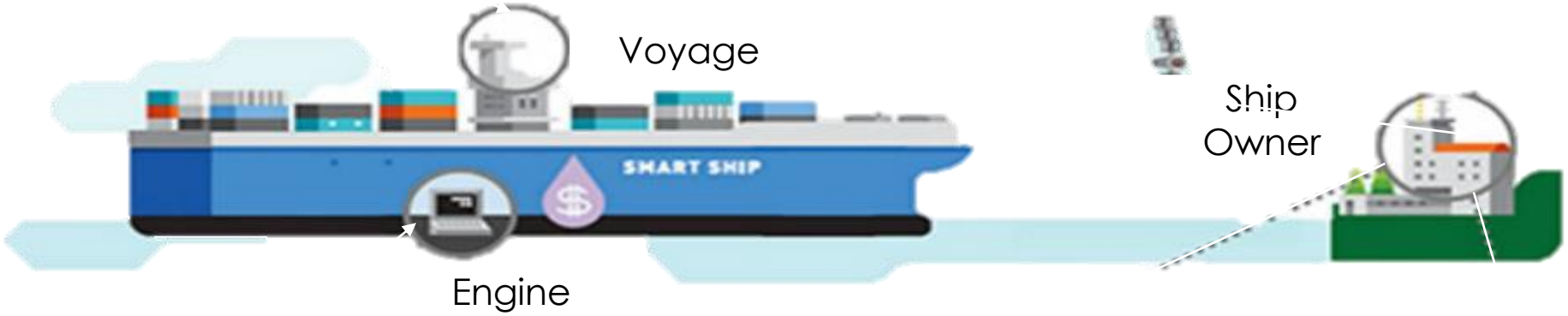


Navigation & security

Specific Tools(cargo & passengers)



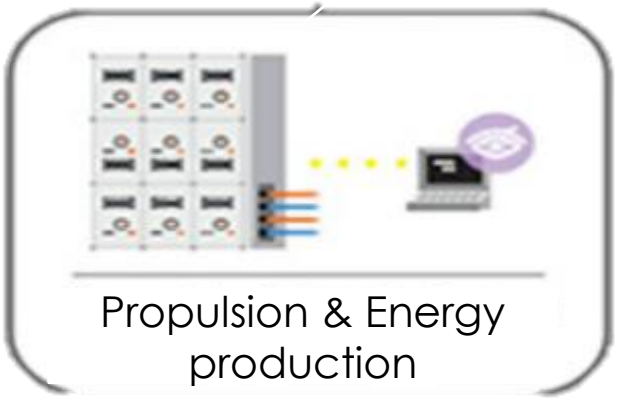
Fleet Monitoring



Voyage

Ship Owner

Engine



Propulsion & Energy production

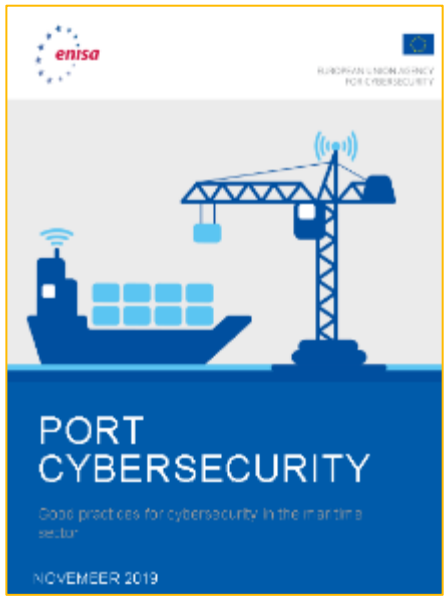
Operational Maintenance

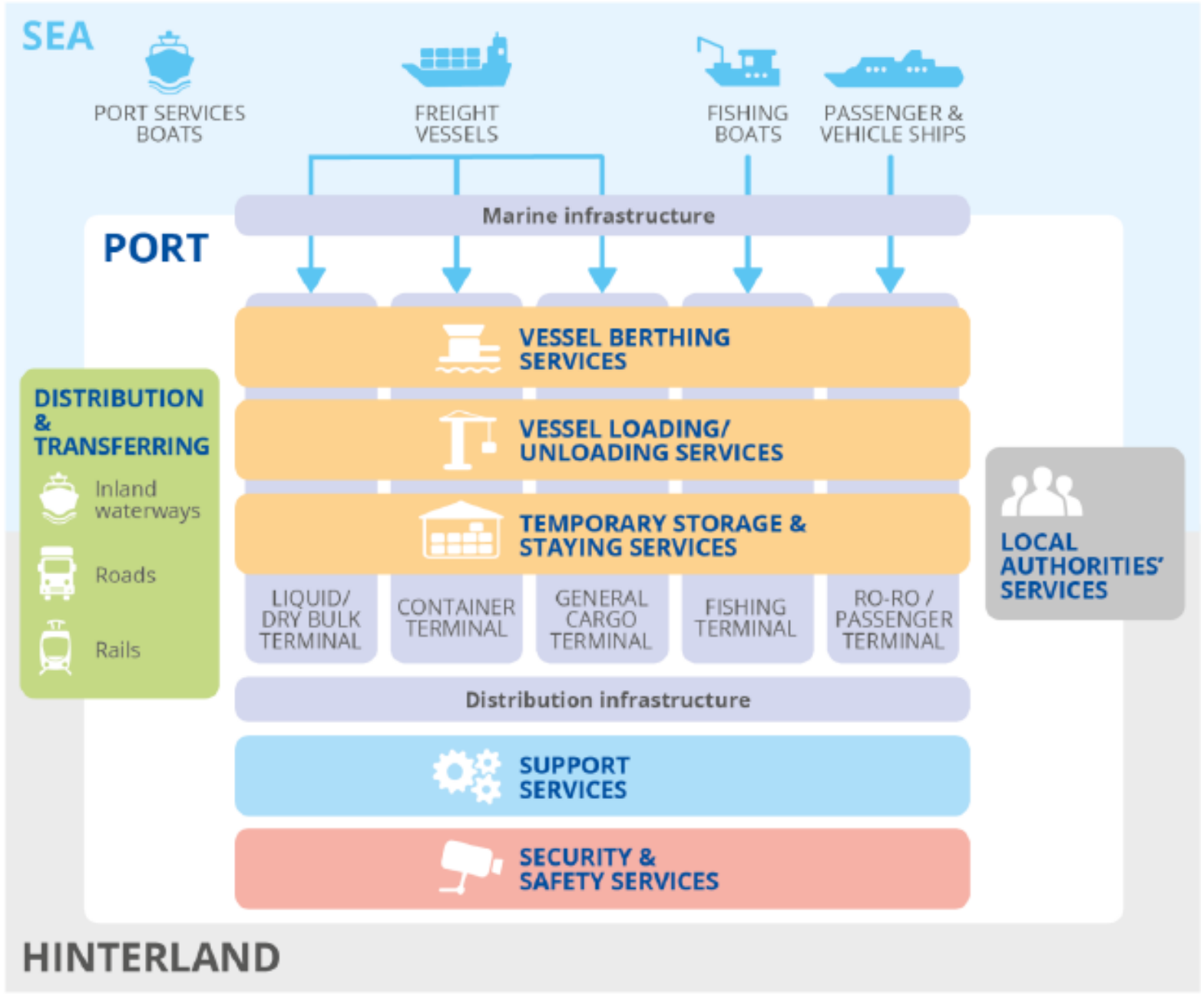
Security Maintenance

Maritime Framework – Technical

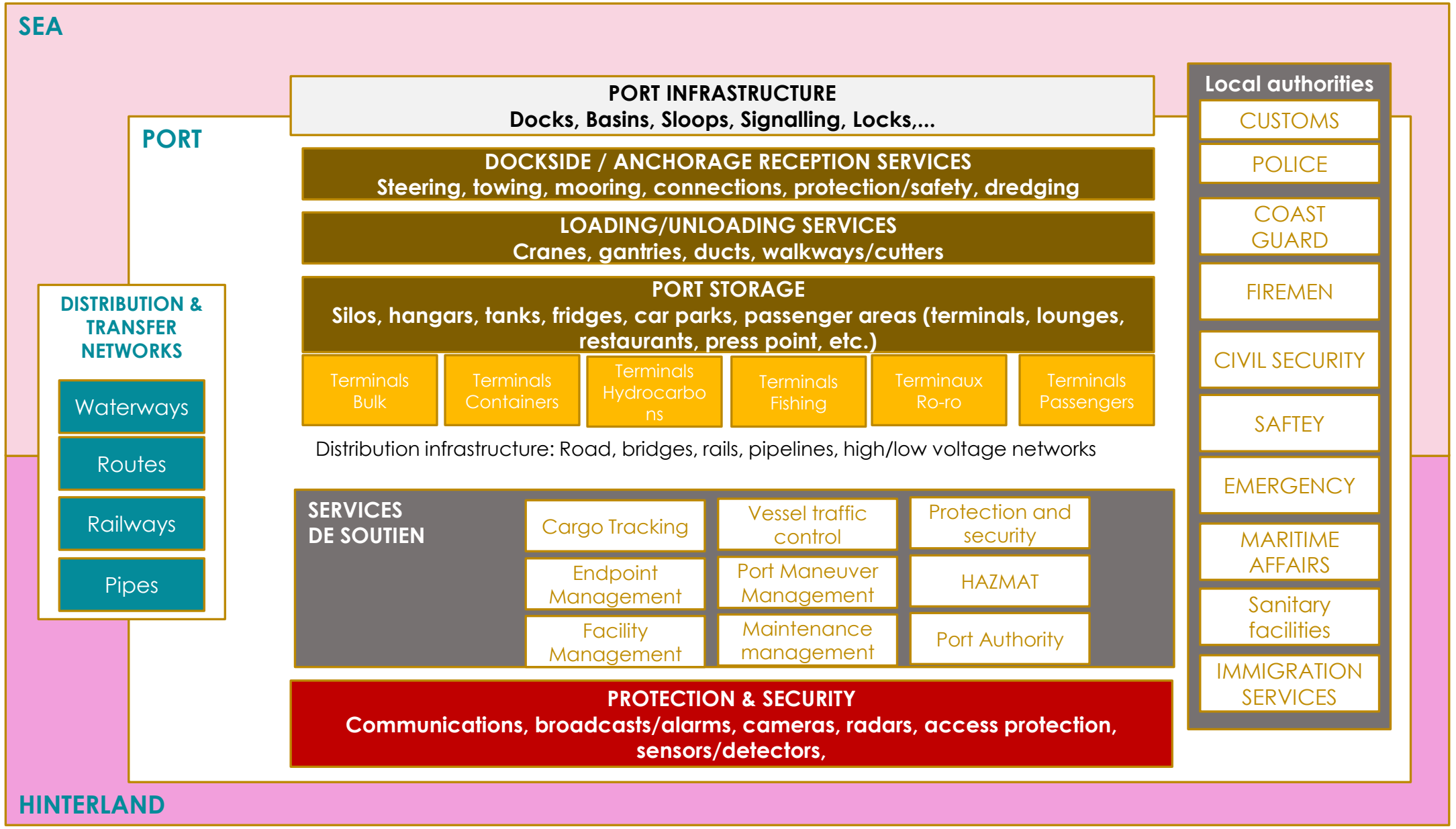
Digitalised Harbor

Cartography

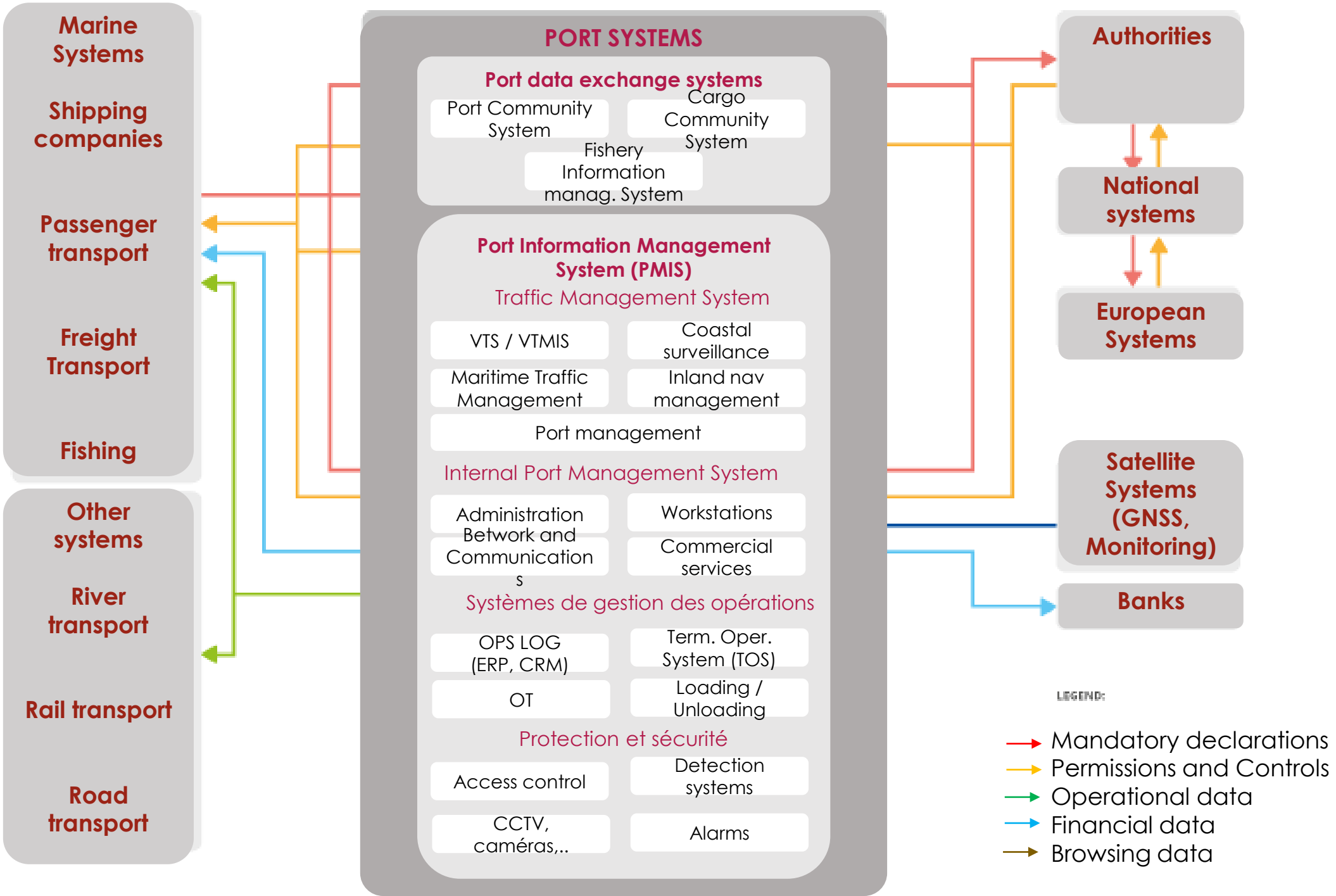




Maritime Framework – Port infrastructure



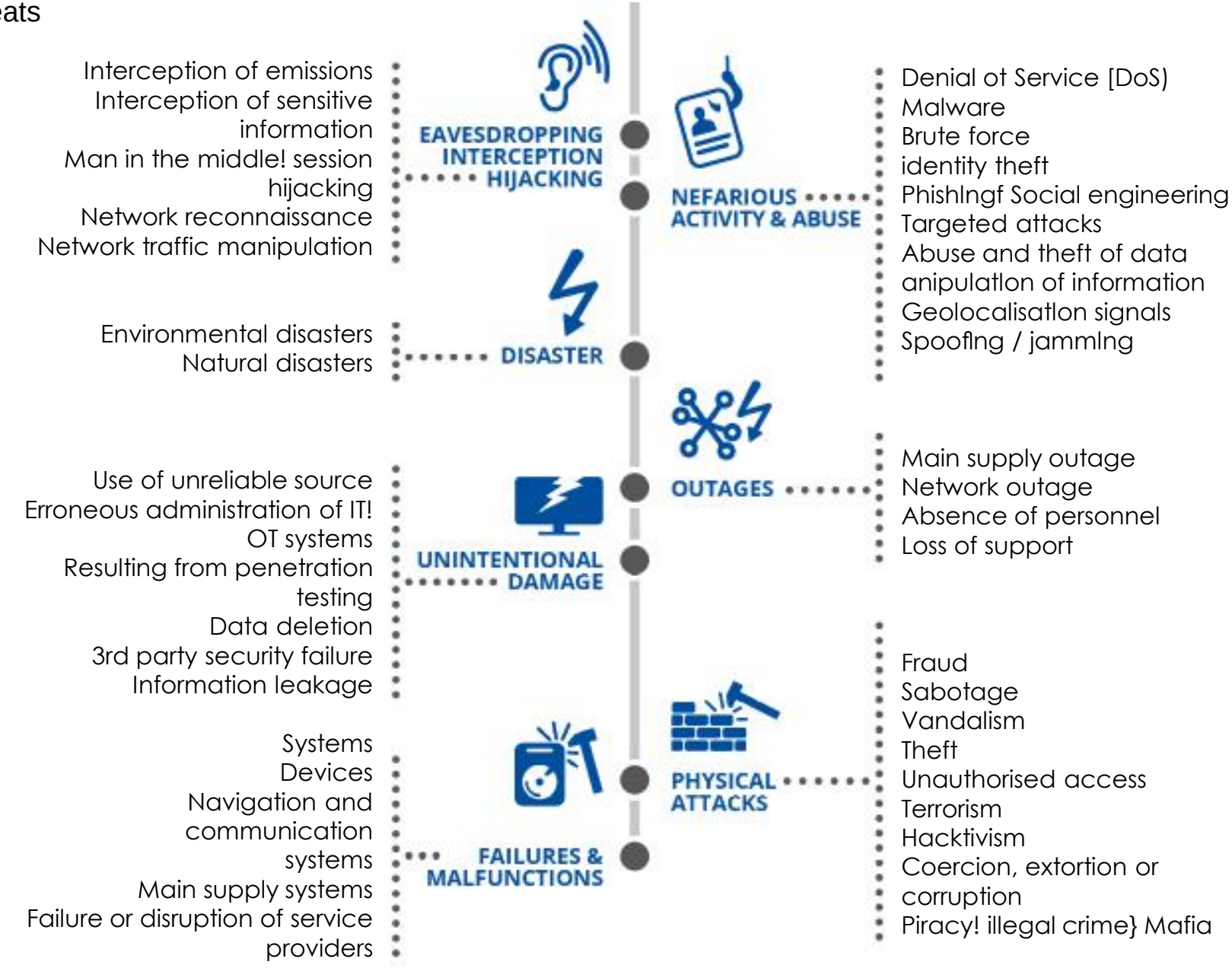
Port systems



Threats

Maritime Domain Threats

Threat Taxonomy

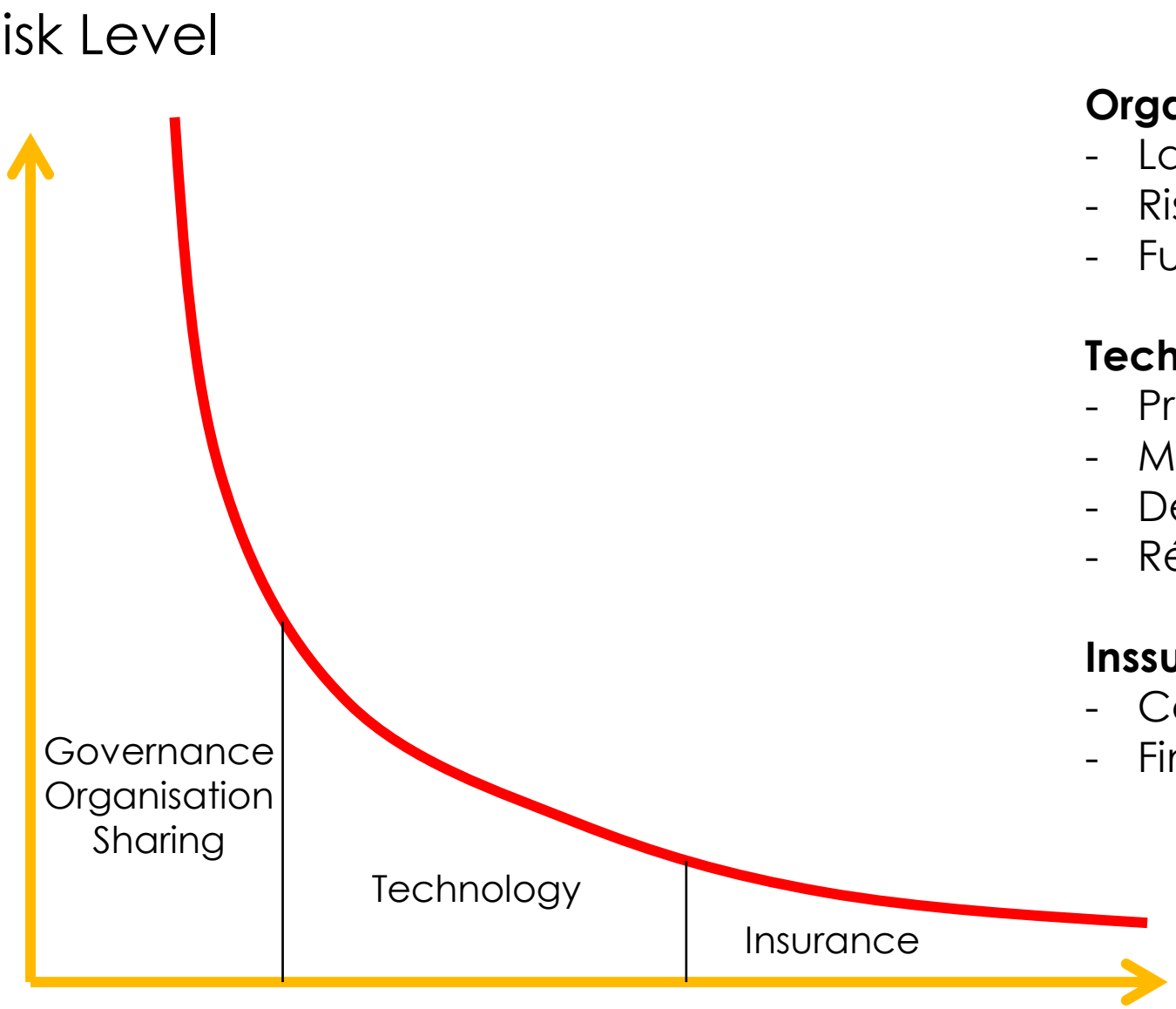


Mitigations of Risks for Critical infrastructrure

Maritime

HARBOURS & MARITIME STAKEHOLDERS

Cybersecurity Risk Reduction strategies and effects



Organisation
- Law / Governance
- Risk analysis
- Functional / sectorial resilience

Technologique
- Prevention
- Monitoring / surveillance
- Detection &incident sharing
- Résilience

Inssurance
- Confidence
- Financial support / reconstruction

QUESTIONS ?

-

BREAK