Garantire la copertura dei rischi legati agli attacchi informatici

UE7- C2 Assicurazione a copertura dei costi causati dagli attacchi informatici ai sistemi informativi

Rischio e assicurazione

- Analisi tecnica (ANSSI)
- Studio settoriale (CFM)
- Analisi dei rischi (BESSE / ANSSI)

SEMESTRE 10					
UE 7 - Attuare una politica di sicurezza informatica efficace		**BC 3**	**45**	*6*	**6**
UE7-A - Definizioni dei concetti di sicurezza e protezione			**15**	**2**	**2**
UE7-A-1	Sicurezza e protezione, due ambiti distinti ma di pari importanza				
UE7-A-2	Cybersicurezza: una visione condivisa tra utenti, progettisti di apparecchiature, reti di trasmissione, servizi di gestione dei dati				
UE7-C - Assicurare il rischio legato agli attacchi informatici			**15**	*2*	**2**
UE7-C-1	Identificare i settori funzionali, mapparli e garantirne l' interoperabilità sicura - Esigenze, constatazioni, analisi				
UE7-C-2	Assicurazione per coprire i costi causati dagli attacchi informatici ai sistemi informativi				
UE7-D - Organizzare i processi per garantire la sicurezza informatica dell'azienda e del suo ambiente			**15**	*2*	**2**
UE7-D-1	Le fasi dell'azione: anticipare e monitorare, reagire e combattere, ripristinare				
UE7-D-2	Gestire la comunicazione interna ed esterna verso i collaboratori, i fornitori, i clienti				

Le capacità informatiche

Les capacités cyber

Certificazione

ISPS, UE, nazionale

Sensibilizzazione

A beneficio del settore

Formazione

Collegamento con gli organismi (ENSM, Marina)

Monitoraggio

SOC – Pattugliamento casuale -/mirato

Analisi dei rischi

A supporto di azioni preventive

Analisi delle minacce

SOC – Pattugliamento casuale -/mirato

Capacità di azione

CERT - CSIRT

R & S

Cattedra cyber – PEC

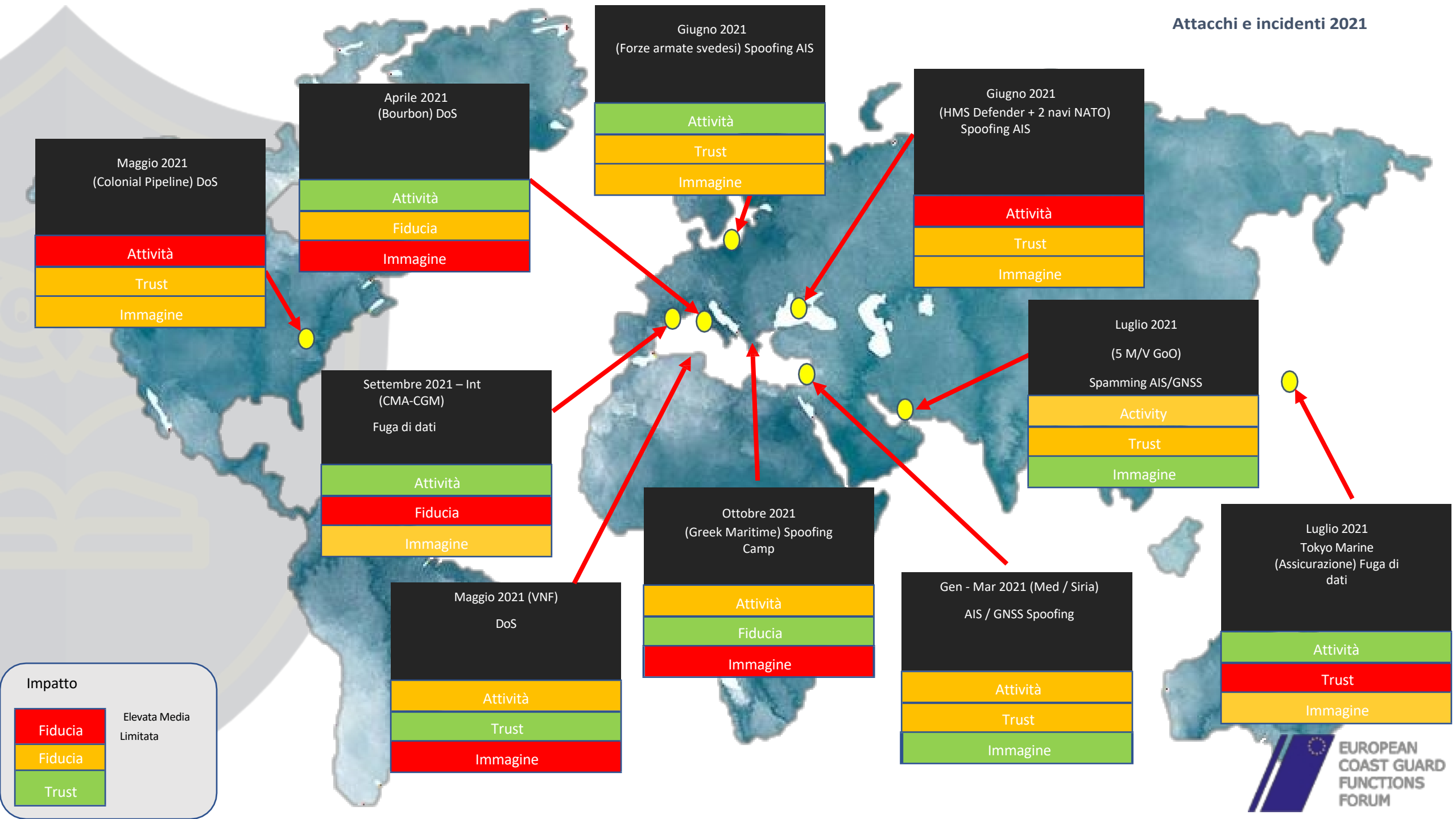
MTES

ANSSI

MINARM

Filiere industriali di sicurezza, del mare

Attacchi e incidenti 2021



EUROPEAN COAST GUARD FUNCTIONS FORUM

Ultimi sviluppi

Un rischio globale

Greek shipowners cyber tricked over Halloween weekend

Adis Ajdin · November 3, 2021 · 2,523 · 1 minute read

To protect Putin, Russia is spoofing GPS signals on a massive scale

GPS spoofing technology linked to Russia has been used almost 10,000 times, tricking ships into being off-grid. It's also used to protect Vladimir Putin and secretive Russian areas

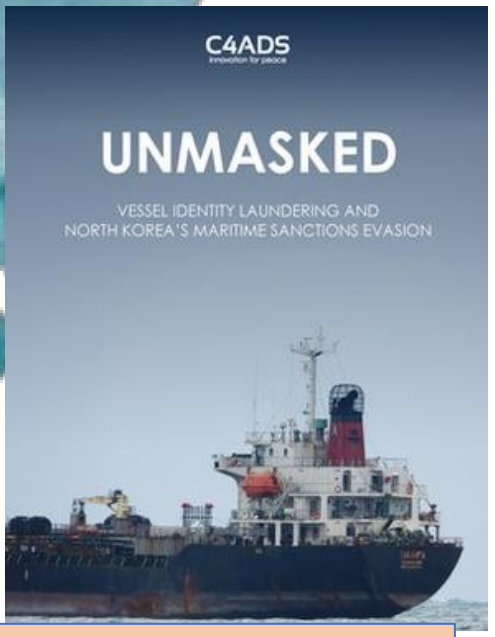
Negli ultimi cinque anni lo spoofing ha colpito centinaia di navi commerciali nelle acque russe.

MAERSK attaccata alle fondamenta

Maersk has suspended a number of crew members after allegations were posted online that a 19-year-old woman was raped aboard one of the company's vessels.

CNN INVESTIGATES

'I was trapped': Shipping giant investigates alleged rape of 19-year-old during federal training program

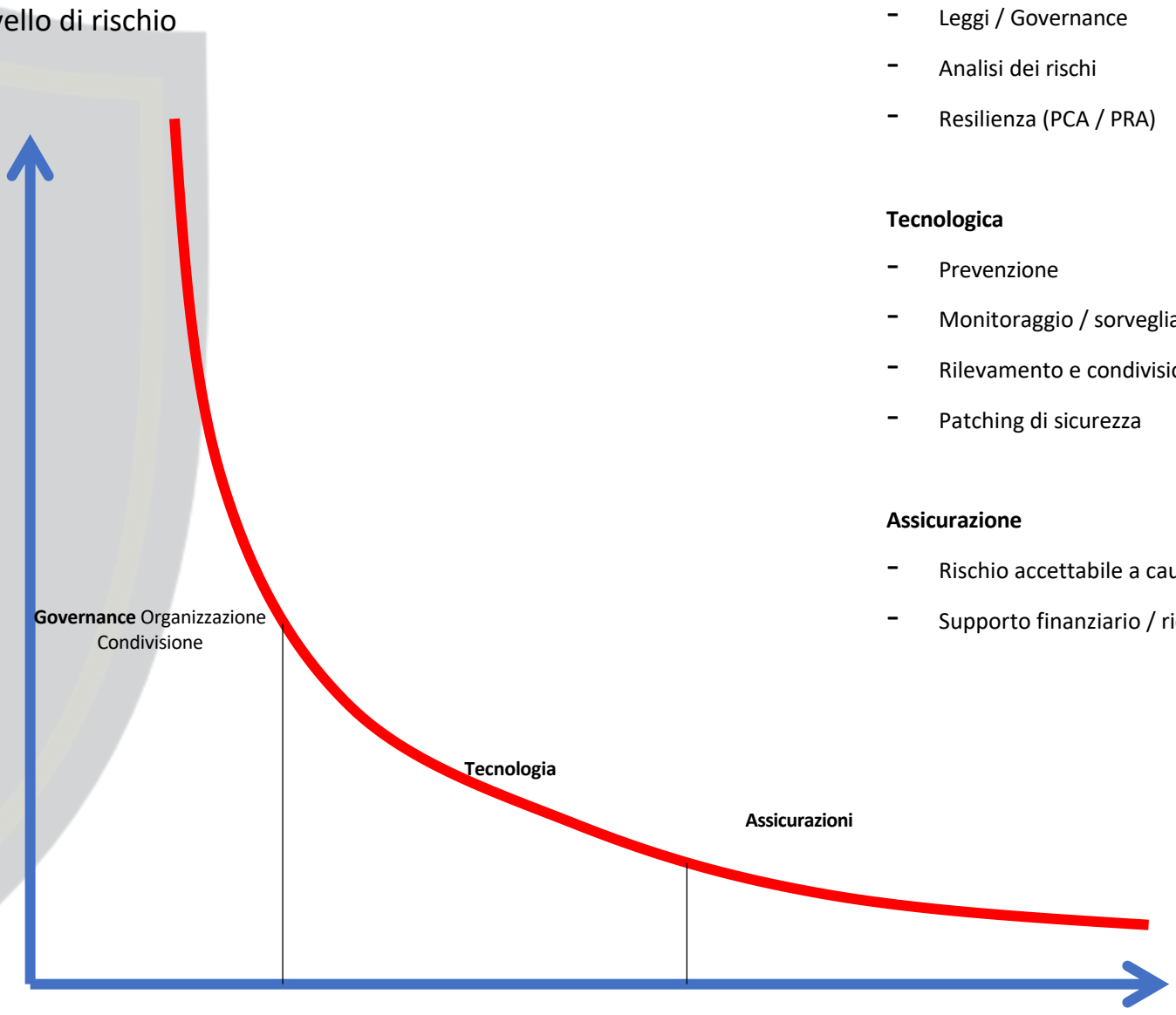


Attraverso **il "riciclaggio dell'identità delle navi"**, coloro che eludono le sanzioni contro la Corea del Nord utilizzano schemi elaborati per creare identità di copertura fraudolente che consentono alle navi soggette a sanzioni di operare impunemente, in alcuni casi per anni (ad esempio: MV KINGSWAY, sanzionata dal Consiglio di sicurezza delle Nazioni Unite per contrabbando di carburante verso la Corea del Nord
Corea, che ha riciclato la propria identità alla fine del 2018 e ha continuato a operare senza essere individuata per tre anni.

https://splash247.com/new-report-highlights-the-rise-of-vessel-identity-laundering/

Operazioni di informazione Guerra dell'informazione

Riduzione del rischio informatico



Organizzazione

- Leggi / Governance
- Analisi dei rischi
- Resilienza (PCA / PRA)

Tecnologica

- Prevenzione
- Monitoraggio / sorveglianza
- Rilevamento e condivisione degli incidenti
- Patching di sicurezza

Assicurazione

- Rischio accettabile a causa della bassa frequenza
- Supporto finanziario / ricostruzione

Cybersecurity nel mondo marittimo

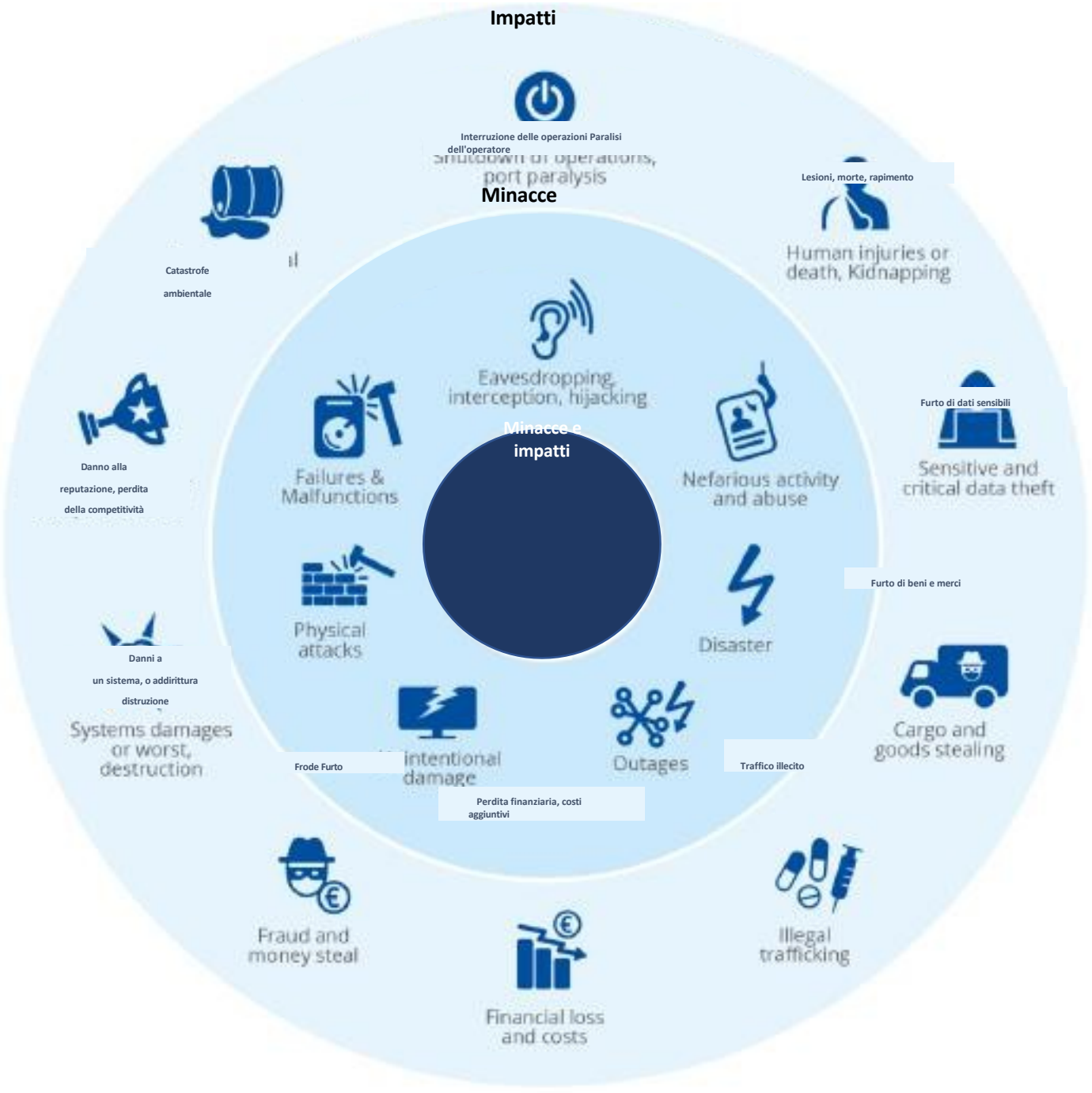
-

Studi

1 – ANSSI

2 – CFM

3 – BESSE / ANSSI



Le analisi dei rischi condotte nel settore, in particolare dall'ANSSI, consentono di identificare diverse minacce applicabili al settore marittimo nel suo complesso. Lo studio presentato all'IMO nel 2017 evidenzia i seguenti 5 ambiti:

- Le informazioni e dei sistemi operativi a a bordo delle edifici e loro vulnerabilità
- L'interconnettività dei sistemi (sia a bordo che a terra)
- Lo sviluppo dell'Internet delle cose (IOT) e della mobilità
- La mancanza di resilienza degli edifici
- La mancanza di formazione e addestramento degli equipaggi di fronte ad atti dolosi

Durante un audit, la DAM ha descritto le misure da attuare per aumentare il

livello di protezione della nave.

In particolare nei settori della fiducia digitale, della governance, della gestione degli accessi e delle fughe di dati, della sicurezza e della tracciabilità delle transazioni, della riservatezza e della continuità del servizio.

Infine, ha condotto un'analisi a seguito della valutazione dei rischi che illustra in modo sintetico i mezzi che possono essere messi in atto per proteggere i sistemi industriali integrati. Questi primi sforzi meritano di essere portati avanti in un quadro definito e con strumenti specifici per il settore.

Altri studi sono stati condotti in particolare da società private, dall'IMO e dalla DG MARE

Sei tipi di minacce

Malware: software dannoso la cui diffusione è incontrollabile

Script kiddy (adolescente disoccupato o, più in generale, aggressore solitario e opportunista):

- Mezzi molto limitati (< 100 €)
- Il gioco (e possibilmente il profitto) come motivazione
- Attacco opportunistico

Dipendente malintenzionato (rancore / avidità):

- Mezzi modesti (< 1.000 €)
- Motivazione principale: danneggiare il proprio datore di lavoro, evitando le vittime
- Discrezione quando possibile
- Facile accesso a tutte le parti della nave

Gruppo terroristico:

- Mezzi moderati (da 10 a 50.000 €)
- Ricerca di vittime umane, danni materiali, forte visibilità mediatica

Impresa criminale:

- Risorse elevate (dell'ordine di milioni di euro)
- Obiettivo di redditività
- Vincoli morali limitati
- Ricerca della discrezione

Stato:

- Risorse quasi illimitate
- Obiettivi di ogni tipo
- Assenza di vincoli morali
- Discrezione necessaria

Sistemi e Vulnerabilità

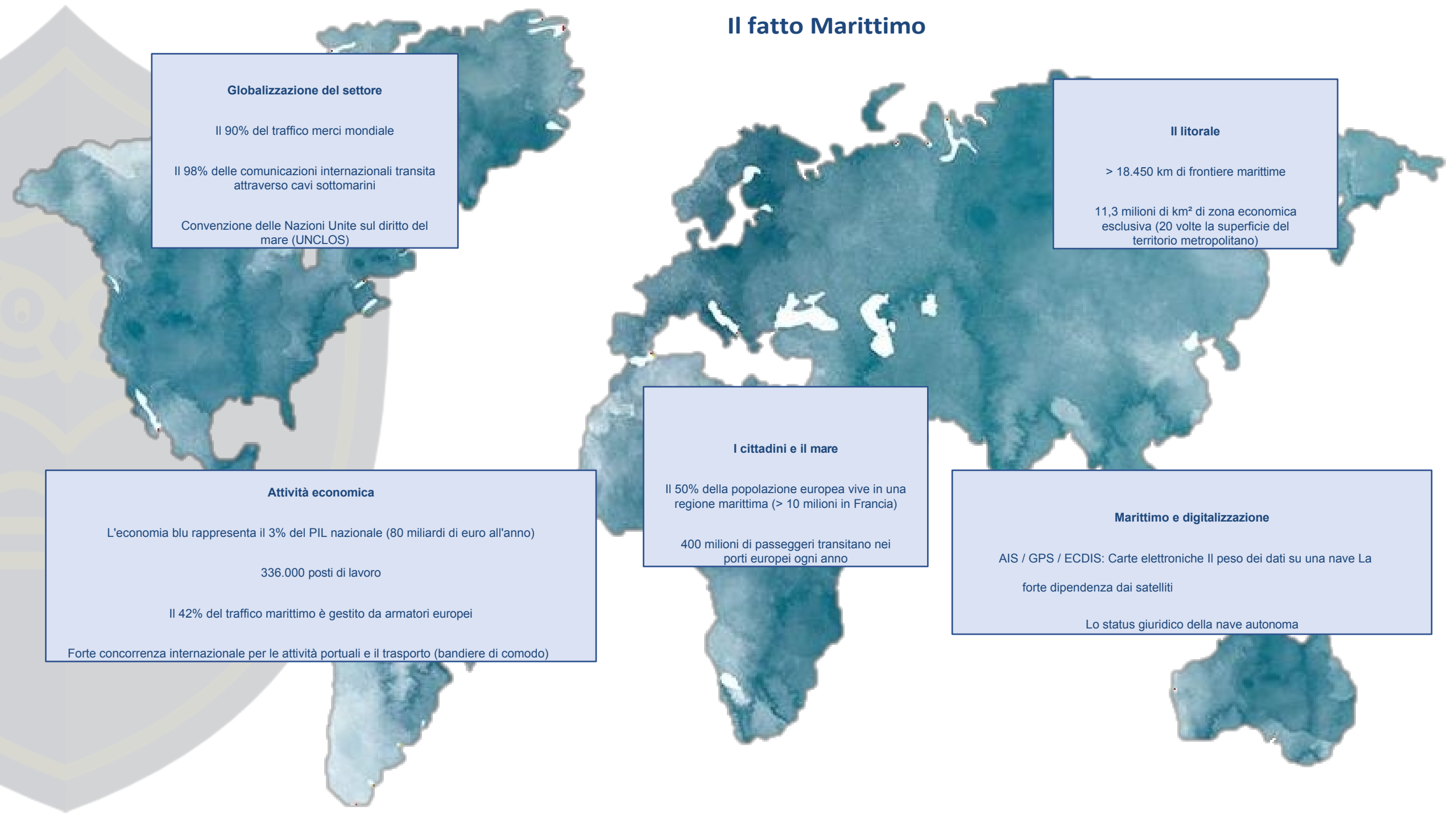
Sistemi, attrezzature e tecnologie dei settori marittimi:

Sistemi infrastrutturali di base Sistemi "back-end" e amministrativi
Sistemi di comunicazione
Sistemi di gestione del carico Sistemi di controllo degli accessi
Sistemi di passerella
Sistemi di propulsione, gestione macchine e controllo potenza Sistemi di manutenzione e gestione passeggeri
Sistemi infrastrutturali di base

Vulnerabilità comuni

- Sistemi operativi obsoleti e non supportati
- Software antivirus obsoleto o mancante (compreso il malware)
- Configurazioni di sicurezza inadeguate e mancata implementazione delle migliori pratiche
- Reti informatiche di bordo prive di segmentazione di rete e protezioni associate.
- Livello di sicurezza insufficiente per le apparecchiature o i sistemi essenziali collegati
- Controlli insufficienti su terzi, inclusi appaltatori e fornitori di servizi.

Il fatto Marittimo



Globalizzazione del settore

Il 90% del traffico merci mondiale

Il 98% delle comunicazioni internazionali transita attraverso cavi sottomarini

Convenzione delle Nazioni Unite sul diritto del mare (UNCLOS)

Il litorale

> 18.450 km di frontiere marittime

11,3 milioni di km² di zona economica esclusiva (20 volte la superficie del territorio metropolitano)

Attività economica

L'economia blu rappresenta il 3% del PIL nazionale (80 miliardi di euro all'anno)

336.000 posti di lavoro

Il 42% del traffico marittimo è gestito da armatori europei

Forte concorrenza internazionale per le attività portuali e il trasporto (bandiere di comodo)

I cittadini e il mare

Il 50% della popolazione europea vive in una regione marittima (> 10 milioni in Francia)

400 milioni di passeggeri transitano nei porti europei ogni anno

Marittimo e digitalizzazione

AIS / GPS / ECDIS: Carte elettroniche Il peso dei dati su una nave La

forte dipendenza dai satelliti

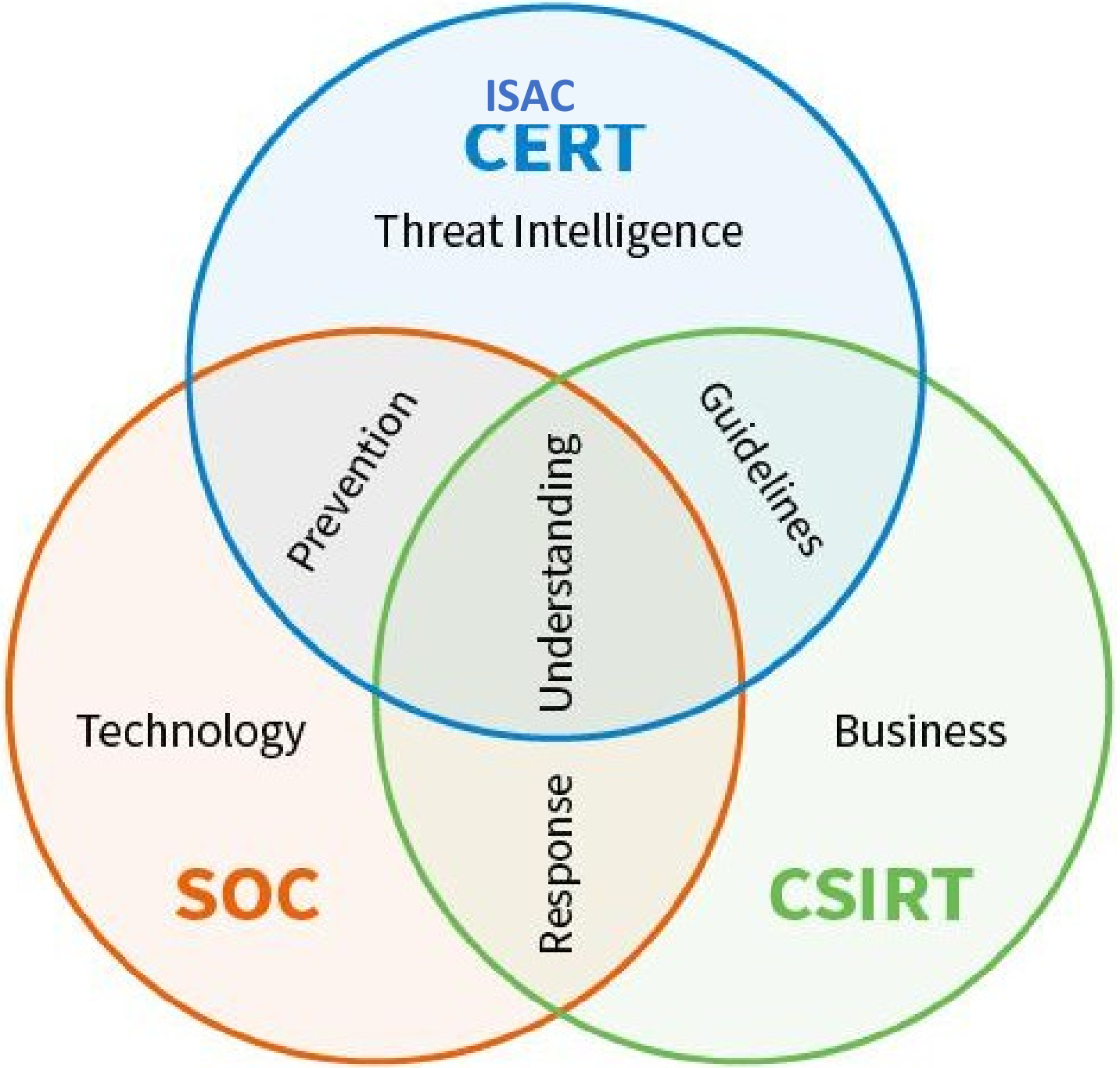
Lo status giuridico della nave autonoma

Domanda posta

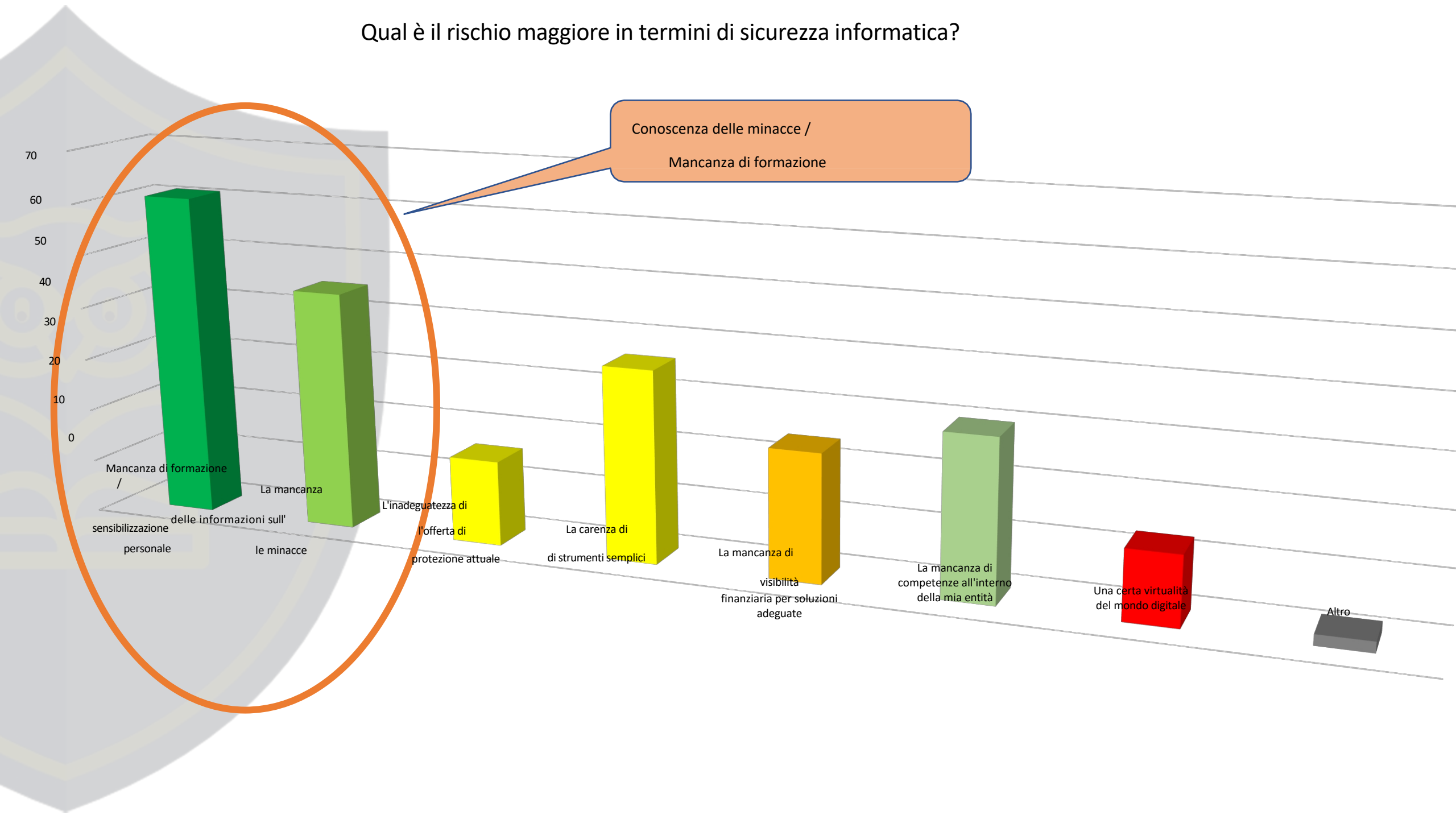
-

Come organizzarsi di fronte alla minaccia informatica

?



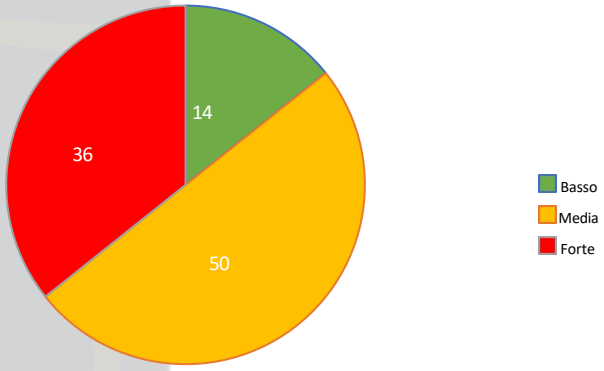
Qual è il rischio maggiore in termini di sicurezza informatica?



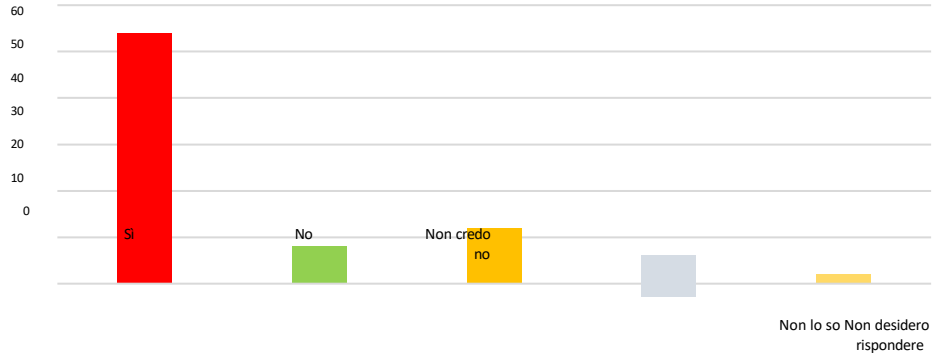
Studio CYBER 2020

Esposizione del settore marittimo - dati 2020 su un campione di 171 organismi che hanno risposto

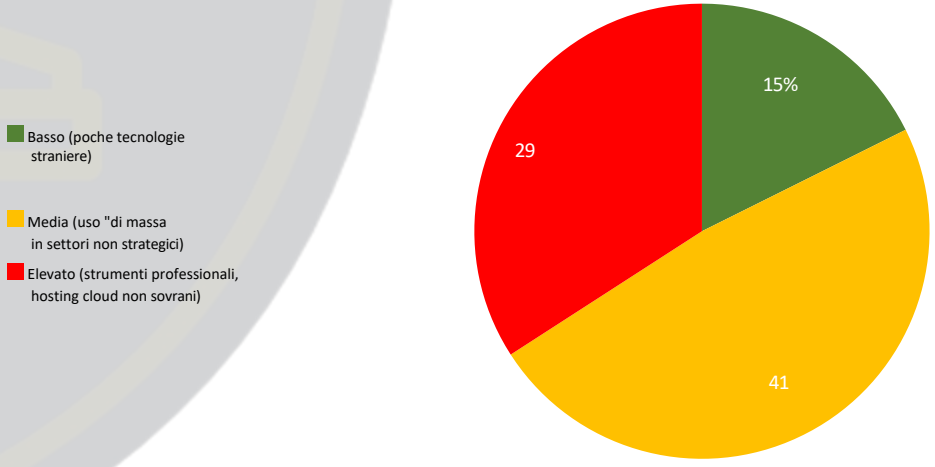
Livello di esposizione stimato alla minaccia informatica



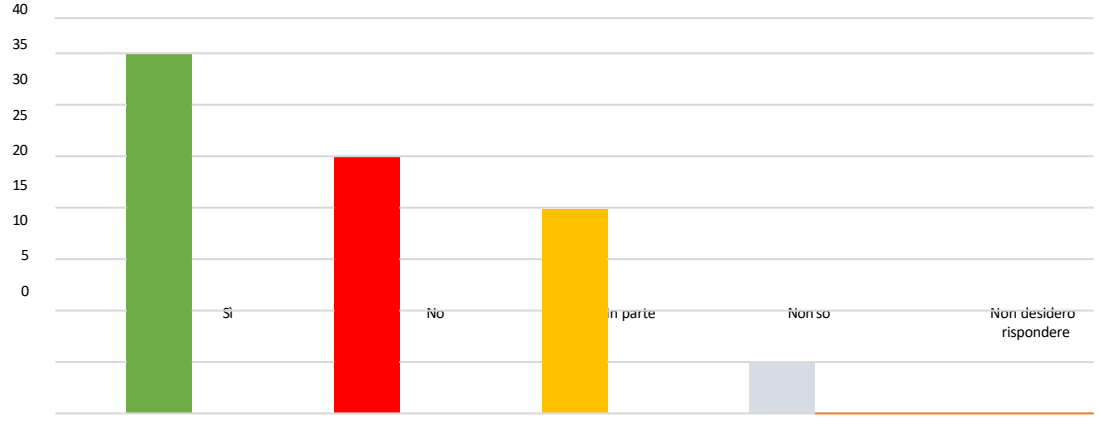
Tentativo di attacco informatico contro l'entità



Dipendenza dalle tecnologie straniere



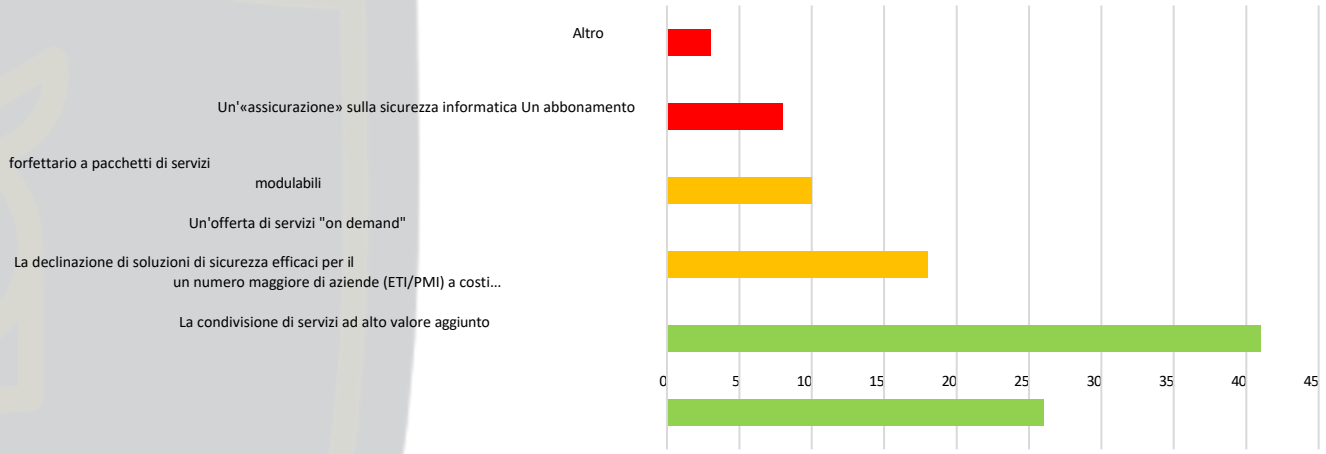
Servizi responsabili della sicurezza informatica all'interno dell'entità



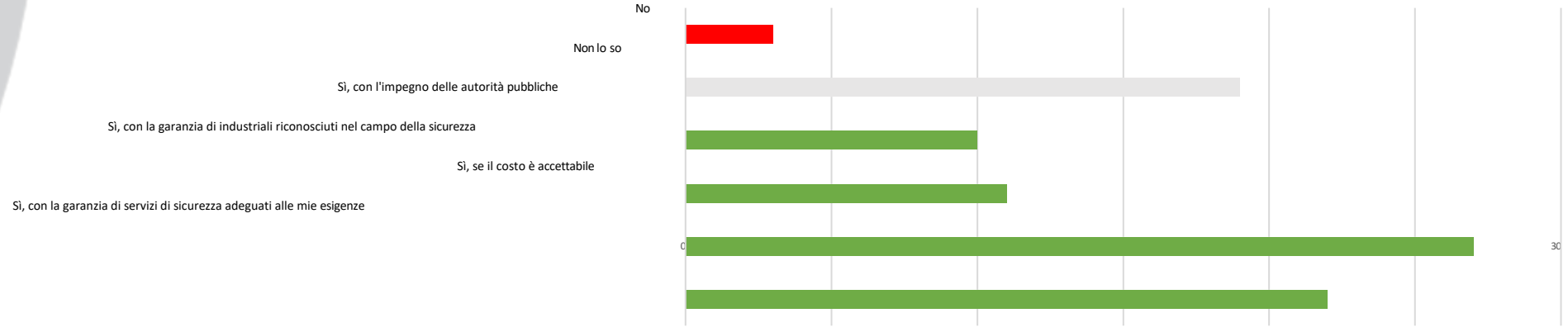
Coordinamento Cyber

Effetti desiderati

I fattori di efficacia di un centro di sicurezza informatica



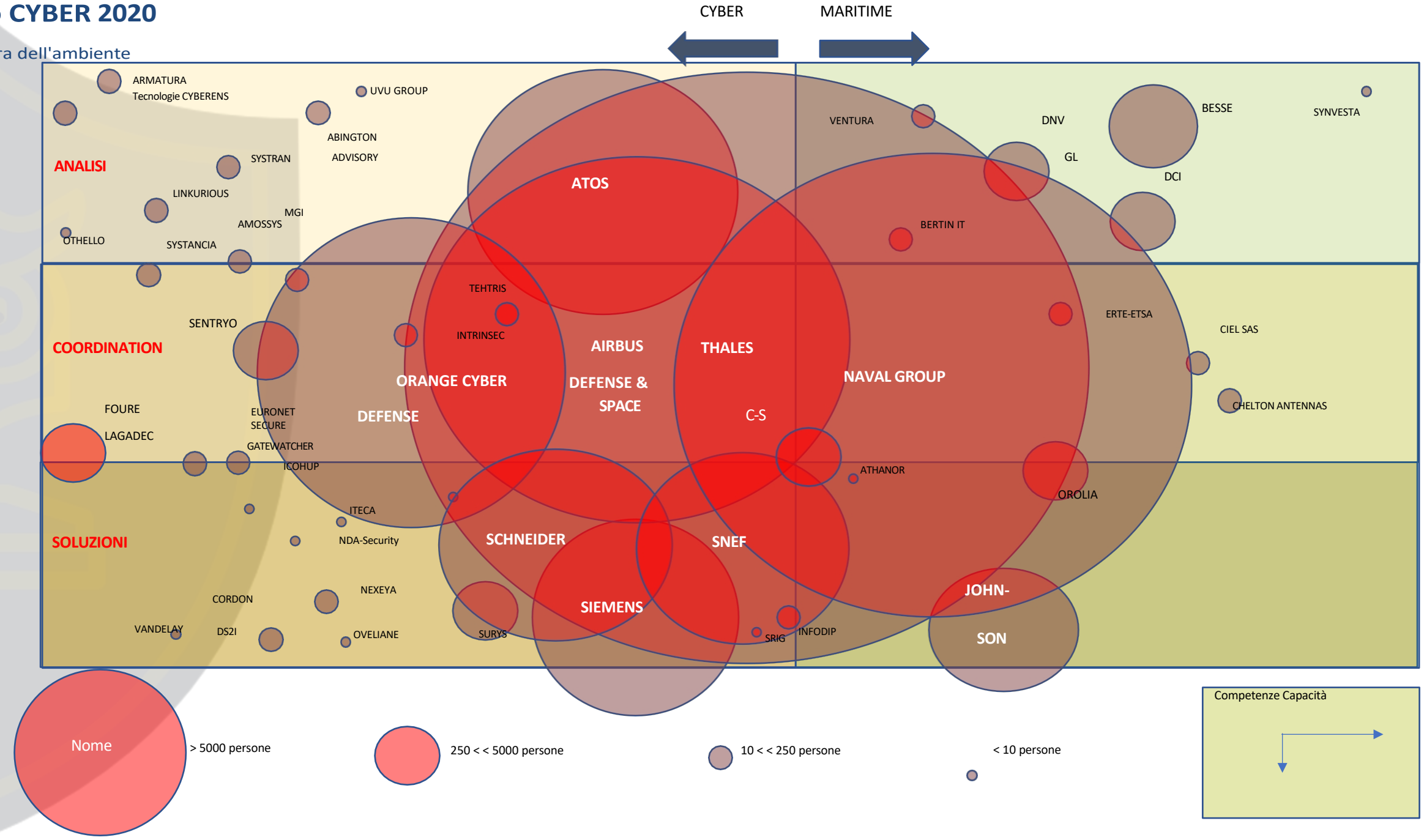
Partecipazione al centro di sicurezza informatica




Lotta
Dare priorità alle azioni relative ai dati e le reti
Formare e sensibilizzare l'intero settore
Prevenire
Dare priorità alla protezione delle tecnologie di comunicazione
Sensibilizzare e formare gli attori della filiera
Monitorare i sistemi critici (sistemi aziendali)
Esigenza Mappatura dei rischi e coordinare l'azione
Dispone di una mappatura dei sistemi critici
Individuare i sistemi critici
Conoscere le minacce / formare le persone
Implementare soluzioni "su misura" per il settore
Dotare il settore di un sistema di "risk assessment" modulabile
Dispone di sistemi omologati e garanzie sugli strumenti
Segnalare gli incidenti
Essere in grado di identificare domani la minaccia percepita oggi
Mettere in atto tematiche unificanti
Governare
Creare una cyber di prossimità
Dispone di una governance forte

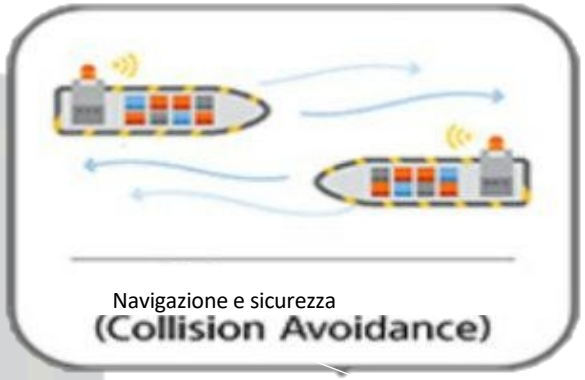
Studio CYBER 2020

Mappatura dell'ambiente

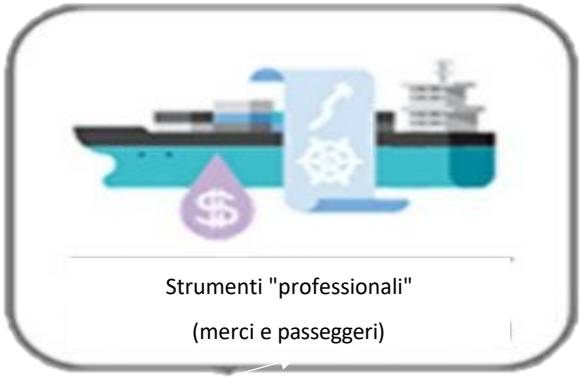


Studio CYBER 2020

Mappatura dei sistemi



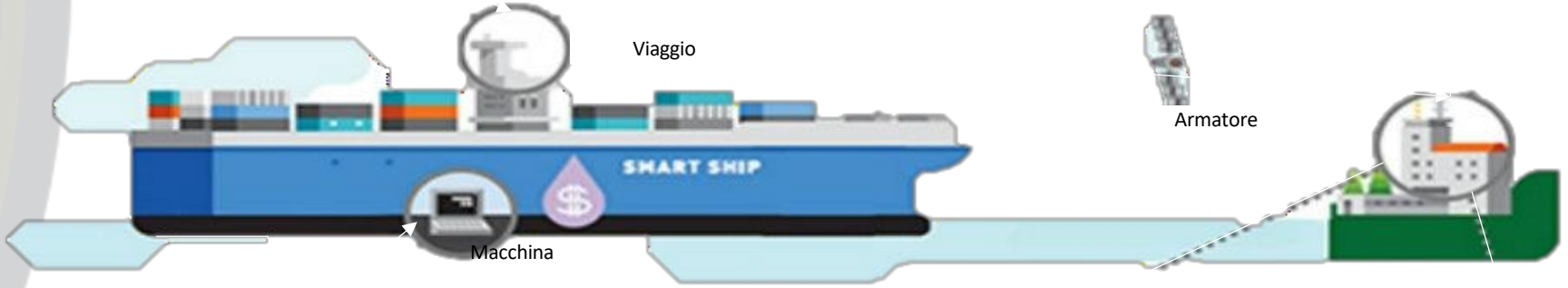
Navigazione e sicurezza



Strumenti "professionali"

(merci e passeggeri)

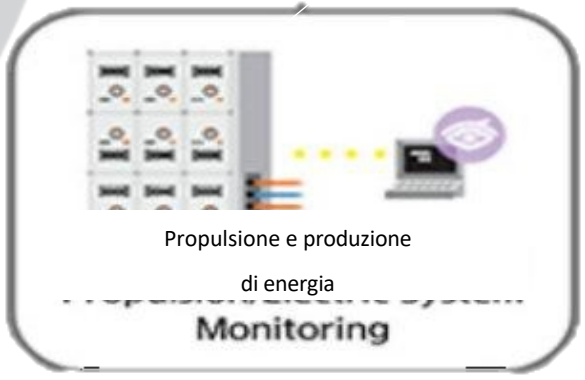
Monitoraggio della flotta



Viaggio

Armatore

Macchina



Propulsione e produzione

di energia

Mantenimento in condizioni

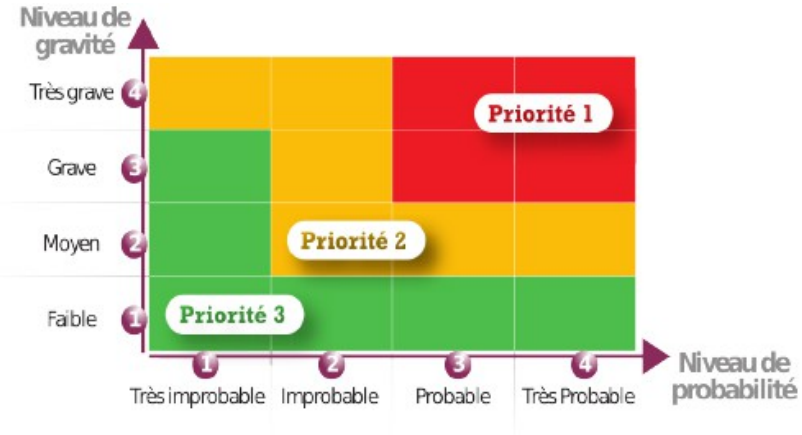
operativa

Mantenimento delle condizioni di

sicurezza

Presentazione da parte del comitato Analisi dei rischi

Objectif



- Analyse de risques **sectorielle**
  - Identifier les risques **représentatifs** et **les plus impactants** pour le secteur

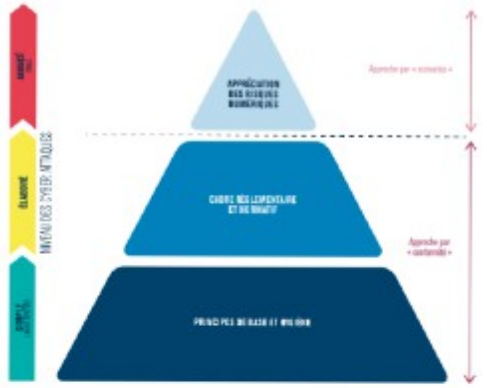
    Opérateur => Secteur => **Missions d'importance Vitale** => **Etat**

  - Disposer d'une cartographie des risques permettant de sensibiliser et d'orienter les actions
  - Recommandations pour compléter la stratégie de cybersécurité maritime du SGMer

Analisi dei rischi informatici nel settore marittimo

EBIOS RISK MANAGER

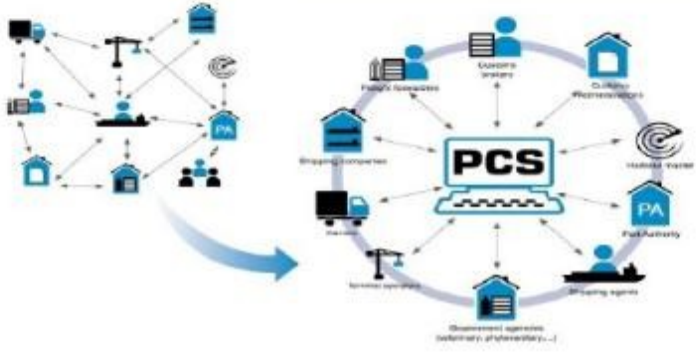
ANSSI



ATELIER 1	ATELIER 2	ATELIER 3	ATELIER 4	ATELIER 5
Cadrage/socle de sécurité	Sources de risque	Scénarios stratégiques	Scénarios opérationnels	Traitement du risque

Périmètre

- Focus sur le « transport maritime » :
  - Compagnies maritimes (marchandises, passagers)
  - Gestion et exploitation d'infrastructures portuaires
  - Fournisseurs de services numériques portuaires (CCS/PCS)



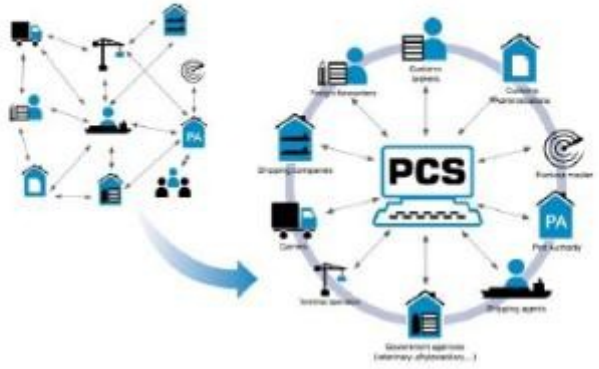
Analisi dei rischi informatici nel settore marittimo

Processus essentiels

Opérateurs	Processus
Compagnies maritimes	*Opération des navires : propulsion, gouverne, navigation, communication, stabilité, énergie…*
	Gestion des marchandises / passagers
	Réservation / Gestion commerciale
	Planification des routes
Ports de commerce	*Gestion des escales*
	Surveillance du trafic (VTS)
	Gestion des infrastructures maritimes (écluses, ponts, bassins...)
	Gestion des marchandises dangereuses
	Gestion de la sûreté et de la sécurité
	GTB – Alimentation électrique
Fournisseur de services numériques portuaires	*Hébergement de services de CCS et PCS*

Evènements redoutés

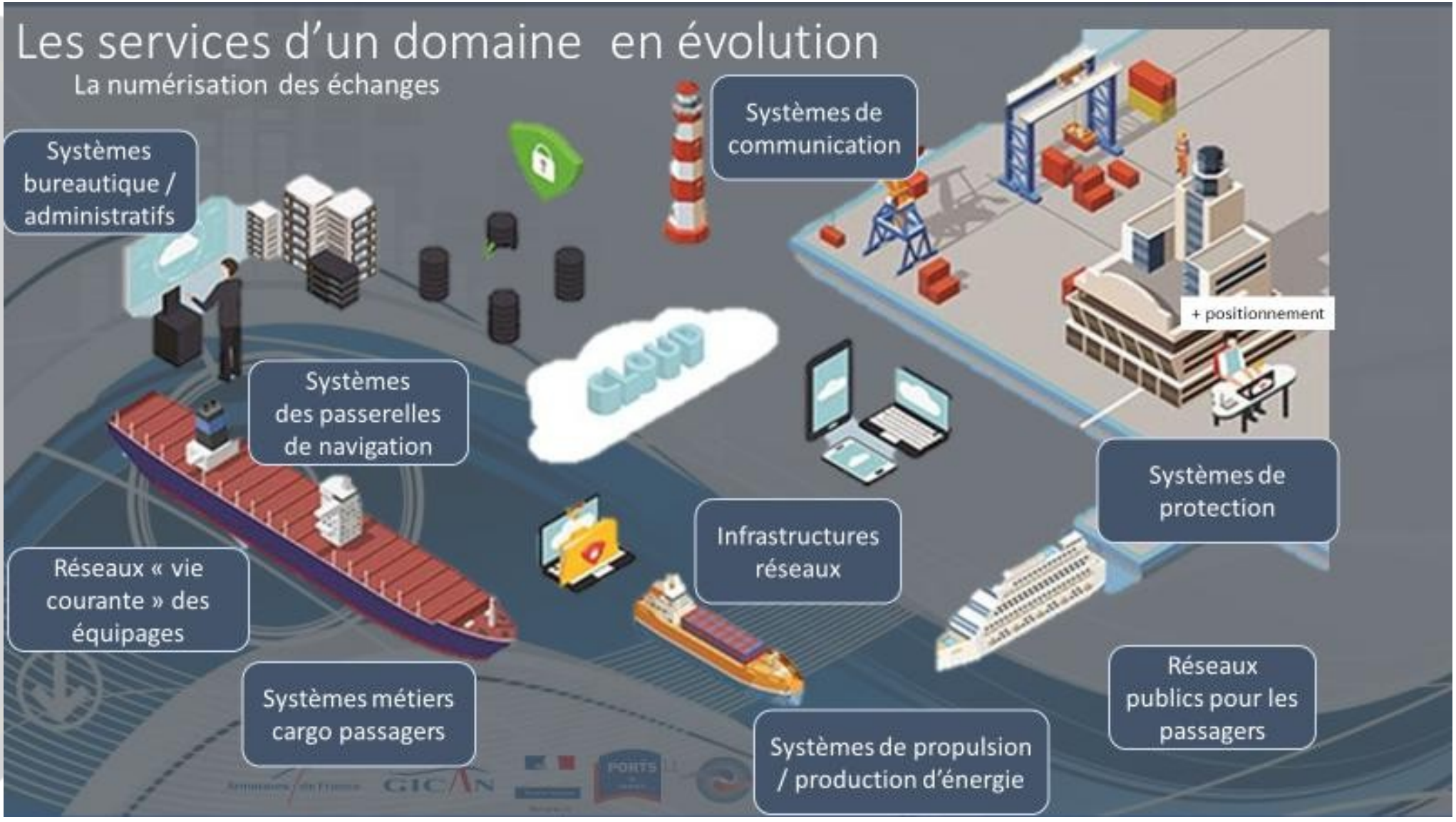
- +40 identifiés dont 9 jugés critiques ou catastrophiques
- Atteintes à la disponibilité et/ou l'intégrité



Scenari temuti

Attacco	Sabotaggio
• Sistemi OT Nave o Flotta • Sistemi di controllo dell'infrastruttura portuale • Sistema di sorveglianza del traffico (VTS) • PCS e CCS	• Sistemi OT Nave o Flotta • Sistemi di controllo dell'infrastruttura portuale • Sistema di sorveglianza del traffico (VTS) • PCS e CCS • Alimentazione elettrica del porto

Analisi e risultati



Strategia di sicurezza informatica del mondo marittimo

Linee strategiche

LE GRANDI LINEE STRATEGICHE

Trasposizione al settore marittimo e portuale dei principi fondamentali della sicurezza informatica che sono stati definiti a livello transettoriale dalla LPM e dalla direttiva NIS su:

- ***Governance (politica generale in materia di sicurezza informatica)***
- ***La protezione delle reti e dei sistemi informativi***
- ***La difesa delle reti e dei sistemi informativi***
- ***La resilienza delle attività***

Definizione di azioni e compiti

Tabella di monitoraggio delle azioni/indicatori

Strategia

Firma congiunta SGM / ANSSI

La sicurezza informatica al centro dei progetti L'equilibrio competitivo

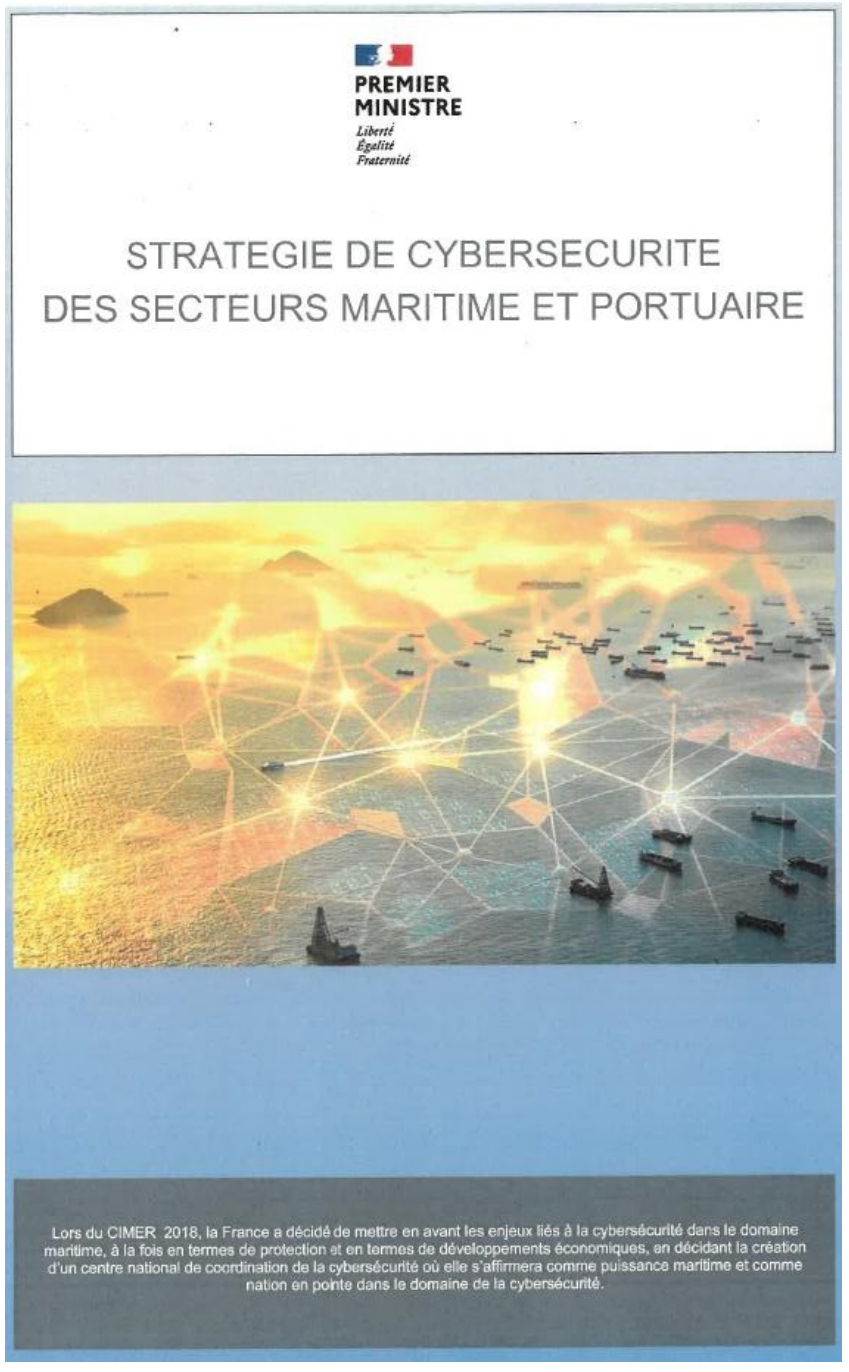
Condivisione delle informazioni

La sfida della complessità dei sistemi

Conciliare la sicurezza informatica e la sicurezza operativa

La copertura dei rischi informatici

Indice



Presentazione della strategia

Piano d'azione (da 1.1 a 1.7)

Settore	N. Azione	Azione	Compito/i	Responsabile	Collaboratori	Scadenza	Commenti	Avanzamento ment
L1: GOVERNANCE	Azione 1.1	Implementare e promuovere la governance della sicurezza informatica marittima	Sviluppare e animare il consiglio per la sicurezza informatica del settore marittimo istituito nel 2019	Segreteria del C2M2	Comitati del C2M2	2019		Realizzato
			Istituire e mantenere un quadro di monitoraggio delle azioni e dei relativi responsabili	Segreteria del C2M2	Comitati del C2M2	settembre 2021	Questa tabella di marcia sarà rivista a ogni riunione del COMEX	Da avviare
	Azione 1.2	Stabilire e mantenere una mappatura dei rischi del settore marittimo	Creare una mappa dei sistemi informativi utilizzati nel settore marittimo e portuale, preliminare alla mappatura dei rischi;	Comitato analisi delle rischi C2M2	Tutti gli attori rilevanti del mondo marittimo	Gennaio 2022	Definizione dell'ambito e approfondimento dell'analisi; condivisione delle informazioni...	avviata
			Produrre e aggiornare la mappatura dei rischi informatici del mondo marittimo.	Comitato di analisi dei rischi C2M2	Tutti gli attori del mondo marittimo	giugno 2022		Da lanciare
	Azione 1.3	Implementare e applicare per il settore marittimo delle indicatori nazionali di sicurezza informatica per il monitoraggio delle politiche e la valutazione della loro efficacia.	Sviluppare indicatori per il monitoraggio delle azioni del presente strategia	Comitati del C2M2	Comitati del C2M2	aprile 2022	Aggiungere una colonna di indicatori alla presente tabella	Da avviare
			Aggiornare il quadro di valutazione dell'evoluzione degli indicatori	Comitati del C2M2	Comitati del C2M2	aprile 2022	Azione permanente	Da avviare
			Effettuare una revisione annuale degli indicatori ed esaminare le azioni da intraprendere di conseguenza	COMEX del C2M2	Comitati del C2M2	aprile 2022	Riunione del COMEX	Da avviare
	Azione 1.4	Coordinare le posizioni e l'azione della Francia presso dei suoi partner internazionali	Contribuire alla redazione di comunicazioni e proposte all'OMI	DGITM/DAM (navi) DGITM/DST (porti)	C2M2	Azione permanente	Il C2M2 coordina, ma il La convalida è interministeriale e la RP presso l'OMI.	lanciato
			Contribuire ai lavori europei attraverso i gruppi di lavoro della CE (ad es. MARSEC, gruppo di cooperazione NIS, ECGFF Cybersecurity WG)	Comitati C2M2	SGMER, MIMER, MTE, ANSSI, Comitato Francia Marittima	Azione permanente		lanciato
	Azione 1.5	Attuare azioni di sensibilizzazione alla alla sicurezza informatica e creare un quadro di formazione rivolto a tutti gli professioni del settore marittimo	Identificare le offerte esistenti e proporle al settore marittima (FR, UE)	France Cyber Marittimo	C2M2 DGITM/DAM (navi) DGITM/DST (porti)	marzo 2022	Aggiornare le guide delle buone pratiche pratiche esistenti	Da avviare
			Sviluppare una piattaforma di sensibilizzazione CYBER marittimo in relazione alle iniziative nazionali e esistenti	France Cyber Marittima	C2M2 DGITM/DAM (navi) DGITM/DST (porti)	giugno 2022	In collaborazione con Cybermalveillance.gouv.fr	Da lanciare
	Azione 1.6	Organizzare e controllare il condivisione di informazioni per tutti gli attori	Pubblicare una newsletter C2M2 cyber all'anno (generalità e attualità internazionale, progetti)	Segreteria del C2M2	Comitati C2M2	Trimestrale	Lanciato nel 2018; formalizzare il ambito di questa lettera con FCM	Realizzato
			Sviluppare e pubblicare bollettini tecnici	France Cyber Maritime	ANSSI (CERT-FR)		Secondo il programma da definire da France Cyber Maritime	Da avviare

Presentazione della strategia

Piano d'azione (2.1-2.4)

Settore	N. Azione	Azione	Compito/i	Responsabile	Collaboratori	Scadenza	Commenti	Avanzamento ment
L2: PROTEZIONE DELLE RETI E DEI SISTEMI INFORMATIVI	Azione 2.1	Analizzare le esigenze di evoluzioni legislative e regolamentari applicabili al settore marittimo	Trarre le conclusioni dall'analisi dei rischi, compresi i riscontri degli incidenti di sicurezza, al fine di definire le necessità di evoluzioni.	Comitato Prospettive e regolamentazione C2M2	France Cyber Maritime, Comitato Analisi dei rischi	Azione permanente		Da avviare
			Garantire il monitoraggio dell'evoluzione dei testi internazionali e delle norme che potrebbero giustificare una modifica dei testi nazionali	Comitato Prospettive e regolamentazione C2M2	DGITM/DAM (navi) DGITM/DST (porti) ANSSI	Azione permanente		avviata
	Azione 2.2	Contribuire a creare un quadro di certificazione/etichettatura dei prodotti e dei servizi che risponda alle esigenze del settore marittimo	Sostenere un processo di certificazione/etichettatura dinanzi all'OMI in collaborazione con le amministrazioni e gli uffici di classificazione sulla base dei lavori esistente	MIMER / DAM	DGITM/DAM (navi) DGITM/DST (porti) ANSSI	2024	Annotare le azioni intraprese durante l'anno	Da avviare
	Azione 2.3	Definire un quadro di riferimento per la sistematica integrazione della sicurezza informatica nei progetti di progettazione e costruzione di navi e infrastrutture portuali	Sviluppare la "cybersecurity by design" presso gli attori industriali	Comitato Prospettive e regolamentazione C2M2	GICAN ANSSI	Azione permanente	Annotare le azioni intraprese durante l'anno	Da avviare
			Integrare la sicurezza informatica nelle riflessioni sullo sviluppo delle navi autonome	Comitato Prospettive e regolamentazione C2M2	DGITM / DAM CLUSTER MARITIME ANSSI	Azione permanente	Sono in corso riflessioni presso l'OMI nei gruppi che lavorano sulle navi autonome;	Da avviare
	Azione 2.4	Condurre progetti specifici per la messa in sicurezza dei sistemi essenziali	Integrare i rischi di interferenza e disturbo del GNSS e le loro conseguenze su sistemi quali l'AIS o informazioni PNT	Comitato analisi dei rischi C2M2	DGITM CNES ANFR	settembre 22	GT interministeriale - Interferenze AIS / GNSS	avviato
			Continuare a garantire la sicurezza dei sistemi di navigazione	Comitato analisi dei rischi C2M2	CNES CCTA	2024		Da avviare
			Contribuire alla sicurezza dei sistemi portuali e di gestione delle merci	Grandi porti marittimi	Francia PCS	2024	Progetto PIA triennale	Da avviare
			Continuare a sviluppare la sicurezza delle reti elettriche dei porti	Grandi porti marittimi	Francia PCS	2024	Progetto PIA su 3 anni	Da avviare
			Promuovere l'implementazione di soluzioni di monitoraggio e rilevamento degli incidenti di sicurezza sui sistemi portuali	Grandi porti marittimi	Francia Cyber Maritime MICA	2024		Da avviare

Presentazione della strategia

Piano d'azione (azioni 3.1, 4.1 e 4.2)

Settore	N. Azione	Azione	Compito/i	Responsabile	Collaboratori	Scadenza	Commenti	Stato di avanzamento
L3: DIFESA DELLE RETI E DEI SISTEMI INFORMATIVI	Azione 3.1	Accompagnare gli attori del settore marittimo nell'attuazione di processi di sorveglianza, rilevamento e risposta agli incidenti di sicurezza informatica.	Promuovere la segnalazione degli incidenti da parte operatori del settore marittimo	France Cyber marittimo	C2M2 MICA Center	dicembre 2021	Esistono già obblighi di segnalazione (LPM, NIS); nel 2018 la DAM ha diffuso una guida a tutti gli armatori	Da avviare
			Sviluppare e istituire meccanismi di raccolta degli incidenti	Francia Cyber marittimo	MICA Center ANSSI (CERT-FR)	Dicembre 2021		Da avviare
			Istituire un CERT marittimo	Francia Cyber Marittimo	MICA Center GENDARMERIA MARITTIMA ANSSI	dicembre 2023		Da avviare
L4: RESILIENZA DELLE ATTIVITÀ	Azione 4.1	Organizzare la resilienza del settore	Implementare e testare i processi di gestione delle crisi;	Segreteria del C2M2	France Cyber Maritime ANSSI	dicembre 2021	Definizione degli obiettivi, dei perimetri e delle interazioni con le esercitazioni esistenti	Da avviare
			Sviluppare il coordinamento tra gli attori e promuovere la condivisione delle buone pratiche.	Segreteria del C2M2	France Cyber Maritime ANSSI	Dicembre 2021		Da avviare
	Azione 4.2	In alternanza e con i settori marittimo e portuale, organizzare esercitazioni di crisi informatica	Mettere in atto una pianificazione delle esercitazioni per i settori marittimo e portuale, in collegamento con le grandi esercitazioni nazionali;	Segreteria del C2M2	France Cyber Maritime ANSSI	Ogni due anni	Attuazione di un programma di esercitazioni per i settori marittimo e portuale.	Da avviare
			Diffondere a tutte le parti interessate l'analisi dei risultati delle esercitazioni e le azioni da intraprendere.	Segreteria del C2M2	France Cyber Maritime ANSSI	Ogni due anni		Da lanciare

**"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."**