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

Sicurezza delle infrastrutture critiche per il settore marittimo

Corso

CSP008_C_M

PRESENTAZIONE DI: 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

Rischi delle infrastrutture critiche marittime

o1. Identificare il rischio di cybersicurezza per le infrastrutture critiche marittime

o2. Corso annuale nell'ambito dei laboratori marittimi.
presenziale - Tolone)

o3. Infrastrutture critiche, OES, parti interessate del settore marittimo

o4. Specificità nazionali - Direttiva NIS

o5. Importanza dei dati (EUCI, Sensibile, ...)

o6. Valutazione e mitigazione dei rischi (ad es. crittografia)

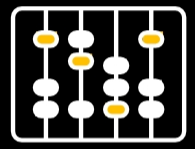
o7. Consulenza C2B
115 rue du maréchal Foch -F83.200 LE REVEST - Francia

Obiettivi: Questo modulo, pensato per gli stakeholder del settore marittimo, mira a identificare i rischi per le infrastrutture critiche al fine di migliorarne la resilienza.

OMS

Mqritime Infrastrutture critiche e OES come identificate nella direttiva NIS

COSA



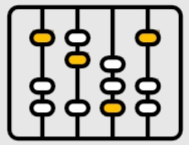
Fondamenti di gestione del rischio di cybersecurity nel settore marittimo

PERCHÉ

Fornire ai partecipanti le conoscenze e le competenze necessarie per gestire i rischi di Cybersecurity.

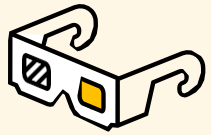
CSP Formazione Logistica: CSP003_ RISCHI DELLE INFRASTRUTTURE CRITICHE MARITTIME

QUANDO



Calendario: Autunno 2024 - Automn 2025

DOVE

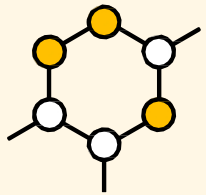


Sede ONSITE

Tolone (Francia)

NMIOTC (Grecia)

COME



- Teoria
- Formazione a mani nude

OMS

Profilo dei partecipanti alla formazione

- Dirigenti e leader
- Professionisti della vita lavorativa
- PMI e dipendenti del settore pubblico
- ~~Professionisti e appassionati di cybersecurity~~
- ~~Sviluppatori di CIS marittimo~~

OMS

Profilo del formatore

- Bruno BENDER
- C2B CONSULENZA
- Ex ufficiale di marina / specialista CIS
- Responsabile della sicurezza delle informazioni
  - NATO
  - A livello nazionale
  - UE
- Dal 2017 Esperto di sicurezza informatica e fondatore di C2B
- PMI specializzata in sicurezza marittima / Cybersecurity a supporto
  - Infrastrutture critiche
  - Operatori di servizi essenziali
  - Società marittime e porti
  - Amministrazioni pubbliche che operano in mare

COSA

Argomenti di formazione

- Qual è la definizione di infrastruttura critica?
- Comunità di utenti
- Architetture tecniche / INFRASTRUTTURE
  - Amministrazioni
  - Descrizione tecnica
- I rischi
- Progettazione dell'architettura di sicurezza
- Implementazione della sicurezza
- Mitigazioni

PERCHÉ

Risultati dell'apprendimento

- Dimostrare una condotta etica e professionale in tutti gli aspetti della gestione delle informazioni e della cybersecurity.
- Comprendere e articolare i concetti chiave e le principi di sicurezza informatica e cybersecurity.
- Comprendere l'evoluzione del panorama delle minacce informatiche e la varietà di attacchi informatici.
- Identifica le minacce, le vulnerabilità e i rischi di cybersecurity per un'organizzazione.
- Riconosce il ruolo del fattore umano nelle violazioni della sicurezza informatica e nelle strategie di riduzione del rischio.
- Capacità di aiutare e selezionare controlli di sicurezza appropriati per proteggere dalle minacce e dai rischi di cybersecurity identificati.

Argomento 1:
Rischi di sicurezza informatica nei settori marittimi

Tratteremo queste competenze

- Introduzione alla sicurezza delle informazioni: Questa sezione introduce il concetto di sicurezza delle informazioni e la sua importanza per le organizzazioni. Si parlerà inoltre dei diversi tipi di risorse informatiche che devono essere protette, nonché delle diverse minacce e vulnerabilità che tali risorse devono affrontare.
- Introduzione alla sicurezza informatica: Questa sezione si concentra sulle minacce specifiche e sulle vulnerabilità esistenti nel dominio informatico. Si parlerà anche dei diversi tipi di attacchi informatici che possono essere lanciati e dei diversi modi per mitigarli.
- La triade della CIA: In questa sezione vengono illustrati i tre pilastri della sicurezza delle informazioni: riservatezza, integrità e disponibilità. Spiegherà il significato e l'importanza di ciascun pilastro.
- Altri modelli di sicurezza: In questa sezione verranno discussi altri modelli di sicurezza che possono essere utilizzati per proteggere le risorse informative. Questi modelli includono il NIST Cybersecurity Framework, lo standard ISO/IEC 27001 e il framework COBIT.

Argomento 2:
Minacce e vulnerabilità

Tratteremo queste competenze

- 1. AIS: cos'è un'infrastruttura critica - Uso legale e specificità
- 2. Descrizione di una struttura di CI comprendente hardware, software e reti.
- 3. I modi in cui le infrastrutture critiche sono minacciate
- Ataackers
- Mitigazioni
- 4. Piani e azioni di resilienza
- Altro

Argomento 3:
Casi d'uso

Tratteremo queste competenze

- 1. Piani nazionali
- 2. Mitigazioni locali
- 3. Istruzione / Formazione
- 4. Indagini e lezioni apprese dal passato
- 5. Minacce e rischi
- 5. Mitigazioni
  - - Tecnica
  - - Organizzazione
  - - Assicurazione

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

Sicurezza delle infrastrutture critiche per il settore marittimo

Corso

CSP0008_C_M

PRESENTAZIONE DI: BRUNO BENDER

Sicurezza delle infrastrutture critiche per il settore marittimo

Argomento 1 - Dati generali

- Quadro marittimo/cibernetico
- Cybersicurezza e tecnologia

Cybersecurity - non solo tecnologia

Servizi

Servizi di protezione

UE CERT-M

Tecnica

Monitoraggio finale/finale
Manutenzione adattiva

Organizzazione

Cyber governance marittima

Valutare e gestire i rischi, segnalare gli incidenti, condividere le analisi.

ETSI GS ISI 00X: "Indicatori di sicurezza delle informazioni (ISI)..."

Legale

Dati commerciali sensibili, dati del personale, posizioni,

Maritime Rischio di cybersicurezza

Obiettivo

Il corso C2B_CSP008 mira a descrivere i rischi di cybersecurity nell'ambiente marittimo e a identificarne le specificità.

L'attenzione si concentra sugli standard e sulle specificità dell'AIS e sulla regolamentazione internazionale. Vengono descritte in dettaglio le vulnerabilità comuni dei sistemi e delle applicazioni AIS/GNSS.

Metodi e esempi di hacking e spoofing di questi sistemi sono dimostrata durante il corso.

Vengono presentati l'analisi dei rischi, i piani di sicurezza, le politiche e i processi, il quadro normativo e le misure di continuità e ripristino degli standard di sicurezza.

Maritime Cybersecurity Rischio

Minaccia di sicurezza informatica per il settore marittimo

- Panorama mondiale
- Attacchi / Incidenti
- Evoluzioni

Rischio nel settore marittimo / Mitigazioni Quali sistemi?

Sicurezza informatica della guardia costiera dell'UE

Risultati - Il proseguimento degli sforzi attuali

Sviluppare l'iniziativa dei workshop ECGFF sulla "Prevenzione degli attacchi informatici nel settore marittimo", avviata dalla presidenza tedesca, e implementare un "Gruppo di lavoro sulla sicurezza informatica della guardia costiera dell'UE".

Necessità di sviluppare un approccio comune alla sicurezza informatica per la comunità dei guardacoste. A tal fine, la comprensione legale, organizzativa e tecnica deve essere ulteriormente sviluppata insieme al miglioramento della cooperazione intersettoriale e transfrontaliera, elaborando linee guida e migliori pratiche di gestione a tal .

Animazione della comunità di cybersecurity della guardia costiera e implementazione di una piattaforma di condivisione delle informazioni dedicata alla cybersecurity e ospitata dall'EMSA.

Convalida consensuale dei termini di riferimento del "Gruppo di lavoro sulla sicurezza informatica della guardia costiera dell'UE".

indirizzata alla Commissione europea (DG MARE).

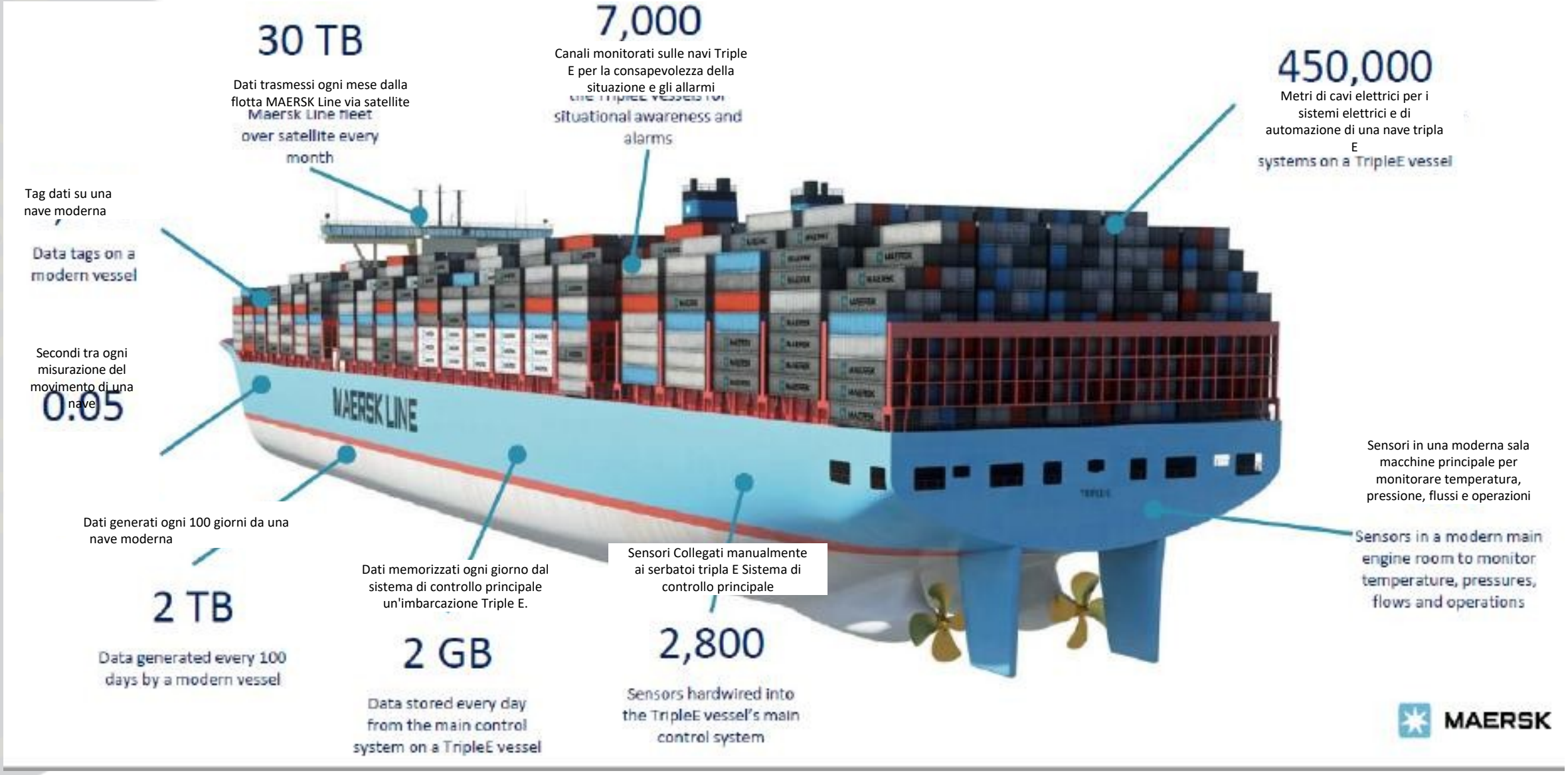
Sostegno a ulteriori miglioramenti dei processi di condivisione delle informazioni per uno scambio tempestivo di informazioni sugli attacchi informatici e sugli incidenti che colpiscono la comunità marittima.

Proseguimento durante la presidenza croata dell'ECGFF (2019-2020).

Cybersicurezza marittima

- **Minaccia di cybersicurezza per il settore marittimo**
- Dati marittimi
- Panorama mondiale
- Attacchi / Incidenti
- I rischi

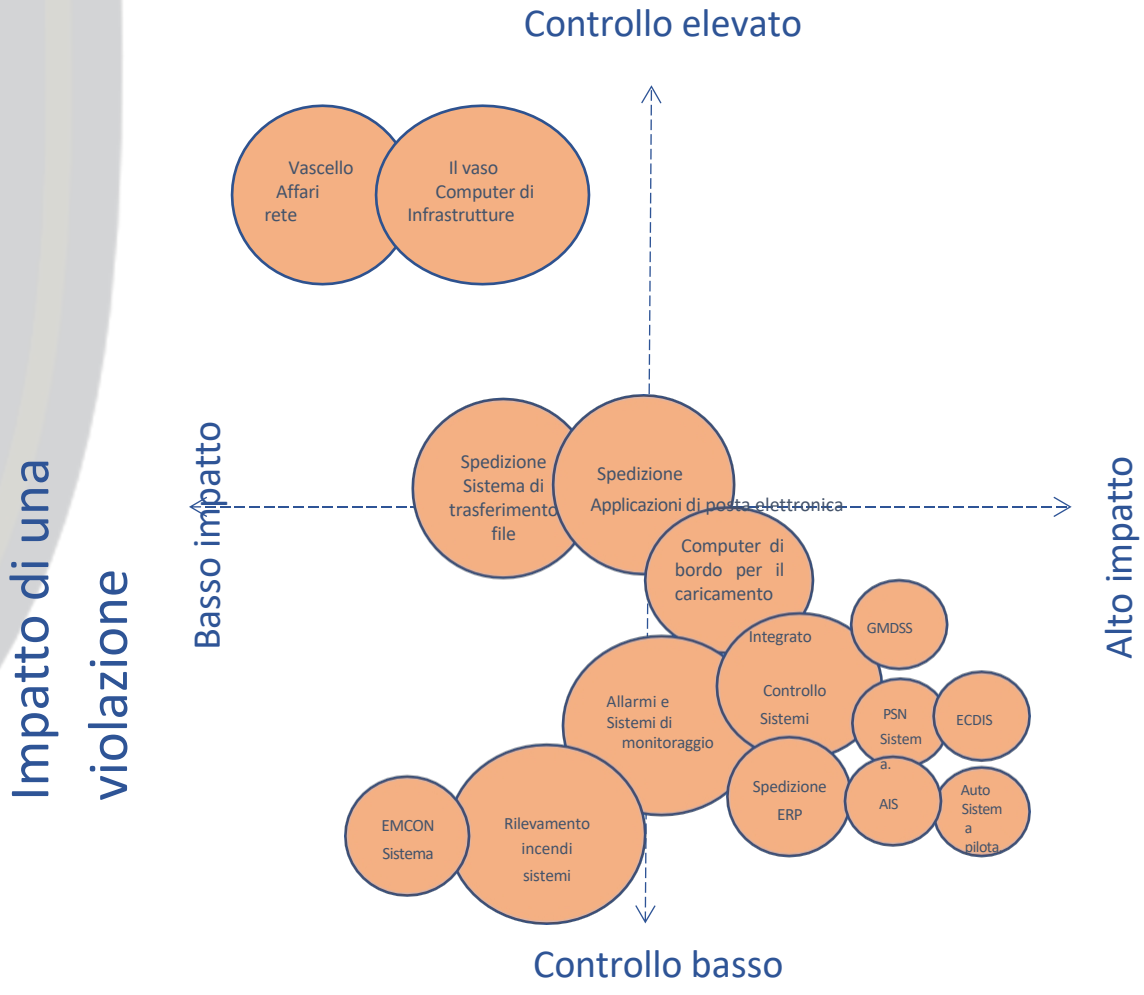
Il rischio di dati nel settore marittimo

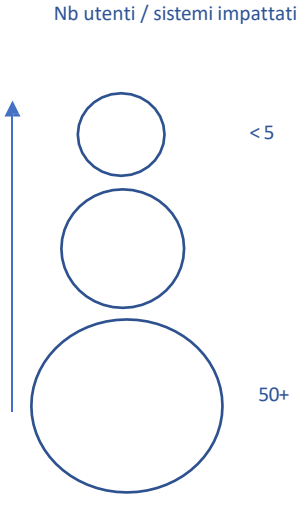


Infrastrutture critiche - Autorità marittime

Controllo sulla sicurezza / Impatto degli incidenti

Controllo della sicurezza da parte dell'armatore





Sicurezza delle infrastrutture critiche per il settore marittimo

Argomento 2 - Minacce e vulnerabilità

- Cartografia dei sistemi marittimi
- Minacce - in tutto il mondo
- Eventi osservati Incidenti

Minacce - Principali attacchi 2020 - 2023

In tutto il mondo

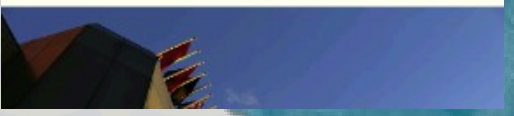
Suspecting Cyber Attack, MSC Reports Network Outage – Update

Mar 2020 - Svizzera (MSC)

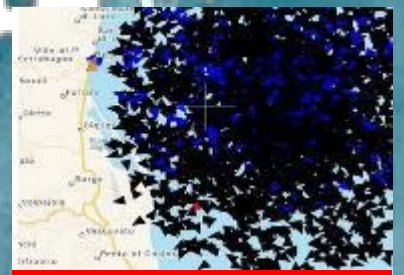
International Maritime Organization
79 323 abonnés
4 h • Modifié •

A number of IMO's web-based services are currently unavailable, including IMO's public website. Service has been restored to the GISIS database, IMODOCS and Virtual Publications. The interruption of service was caused by a sophisticated cyber attack against the Organization's IT systems that overcame robust security measures in place. IMO IT technicians shut down key systems to prevent further damage from the attack. The IMO is working with UN IT and security experts to restore systems as soon as possible, identify the source of the attack, and further enhance security systems to prevent recurrence.

Voir la traduction



Settembre 2020 -
Int (CMA-CGM)



Dic 2019 - Elba
(Spoofing AIS)

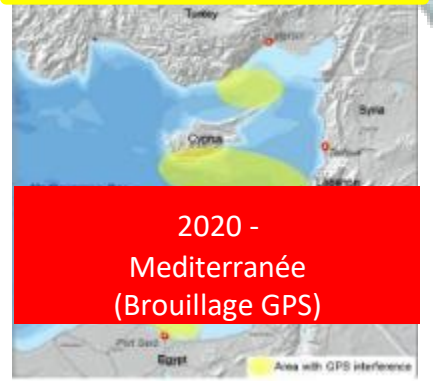
Apr 2020 - Ormuz
Bandar Abbas

Med Europe Terminal

Actualités

/!\ ATTENTION CYBER ATTAQUE /!\

Marte 2020 -
Marsiglia / FOS -
Attacco regionale



2020 -
Mediterranée
(Brouillage GPS)

Gennaio 2020 - Cina
(Spoofing AIS)

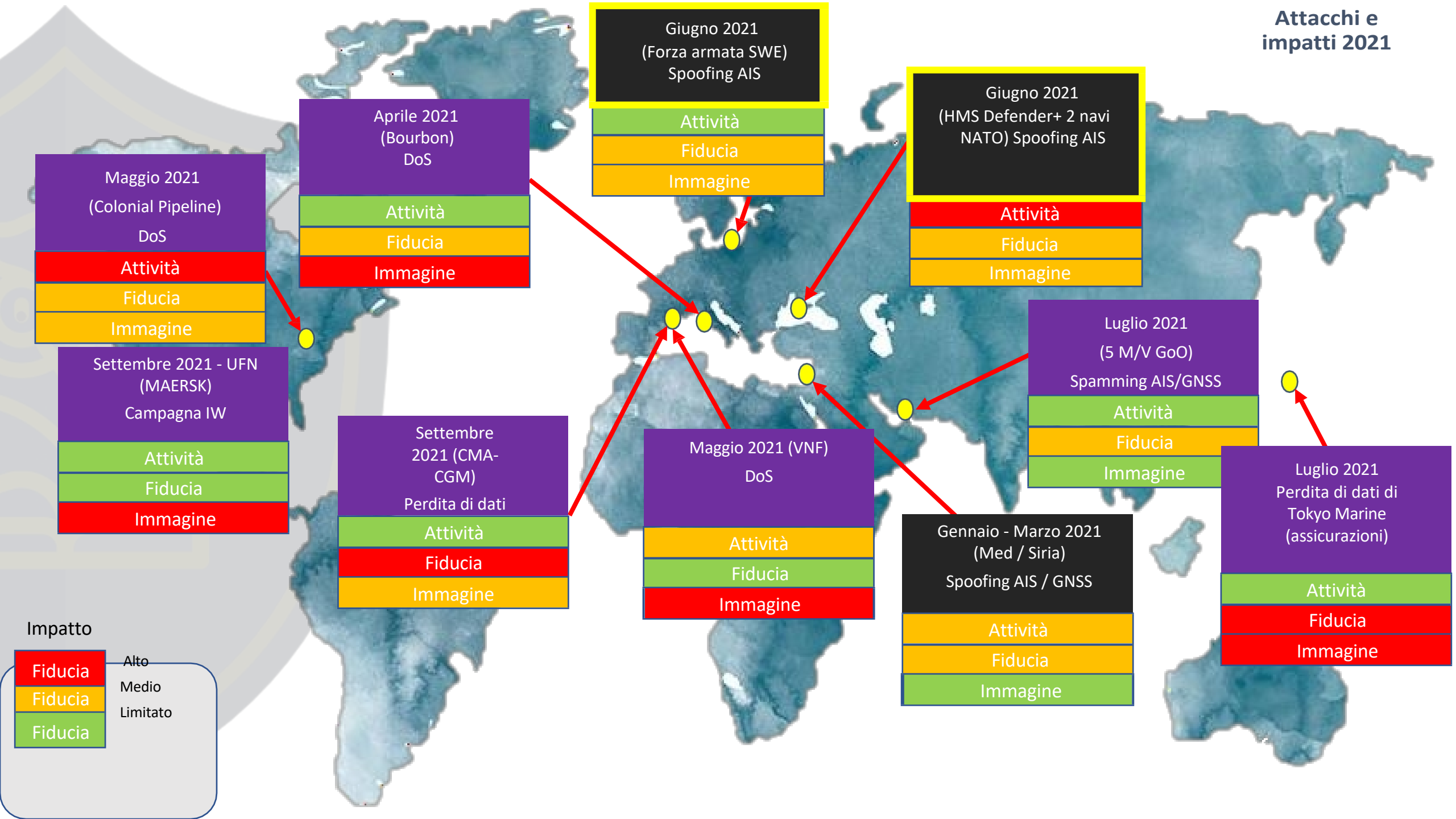
Maggio 2020 - California (Spoofing A

Settembre 2020 -
Int (GEFCO)

Attacchi / incidenti (2020 - 22)

Entità	Data	Impatto	Analisi
Porto di Bandar Abbas	2020	Impossibilità di implementare terminali di carico e scarico	Il **bersaglio** deliberato **di un porto "non critico" da parte di un paese** in un attacco preventivo che ha portato a una risposta immediata.
MSC	2020	Servizi inutilizzabili (>12 ore) Pagina web e interfaccia clienti inaccessibili per diversi giorni in alcune zone	**I servizi ospitati localmente** hanno permesso all'operatore di continuare a operare in alcune regioni
TERMINALE MED EUROPE	2020	Servizi Internet bloccati che hanno avuto un impatto sul portale web e sulla messaggistica.	L'operatore marittimo è stato la **vittima collaterale** di un attacco alla Regione meridionale durante il contenimento della
GNSS/AIS	2018 - 2020	Saturazione dei ricevitori AIS (osservata nel Mediterraneo nel 2019, in Cina e negli USA nel 2020) Disturbo permanente del GPS nel Mediterraneo orientale, in Cina e nel Mar Nero	L'interferenza o lo spoofing (saturazione) dei sistemi GNSS/AIS rappresenta un **pericolo** reale **per la navigazione**. Osservabili nelle loro forme più crude, gli attacchi ai sistemi GNSS/AIS possono finire per **distorcere tutti i dati marittimi**.
CARNEVALE	2020	Perdita dei dati dei clienti e dei dipendenti. Perdita di attività sulla crociera (prenotazioni)	Classico attacco ransomware che ha crittografato parte dei sistemi e dei dati del CIS e bloccato l'attività per diverse ore.
CMA / CGM	2020	Dati e servizi inaccessibili a causa di Cryptolocker Perdita di clienti	L'attacco è stato risolto in più di due settimane da specialisti **che non avevano familiarità con il CIS dell'azienda**. La comunicazione deve concentrarsi sulle priorità degli operatori.
BENETEAU	2021	Attacco ai sistemi e perdita di dati	BENETEAU ha subito un primo attacco nel 2018 e ha perso i dati (liste di clienti) una seconda volta in meno di 3 anni.
BOURBON	2021	Attacco al sistema di sfruttamento principale	Problemi di gestione dei cambi di equipaggio e dell'attività giornaliera e rapporti per le navi
GAZOCEAN	2021	Presidente Rip-Off	Los finanziario
VNF	2021	Attacco al sistema informativo principale	Sistema di gestione bloccato per diversi giorni
Porto di Abidjan	2021	MATRICE Ransomware	Segnalato un impatto limitato sul traffico marittimo dopo una reazione coordinata
DNV-GL	2020	Spiare uno Stato - Furto di dati Immagine della società spellata	Le società di classe sono spesso esposte a questo tipo di rischio a causa delle informazioni che stanno accedendo

Attacchi e impatti 2021



CMA / CGM Attacco 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

L'indagine sul cyberattacco a CMA CGM sta facendo rapidi progressi Se la maggior parte delle indagini sui ransomware non riesce a identificare gli hacker, la polizia informatica ha arrestato in Ucraina i sospetti dell'attacco che ha preso di mira il vettore marittimo CMA CGM nel 2020. L'indagine in corso conferma le prime piste sul Ragnar gang Locker. [...]

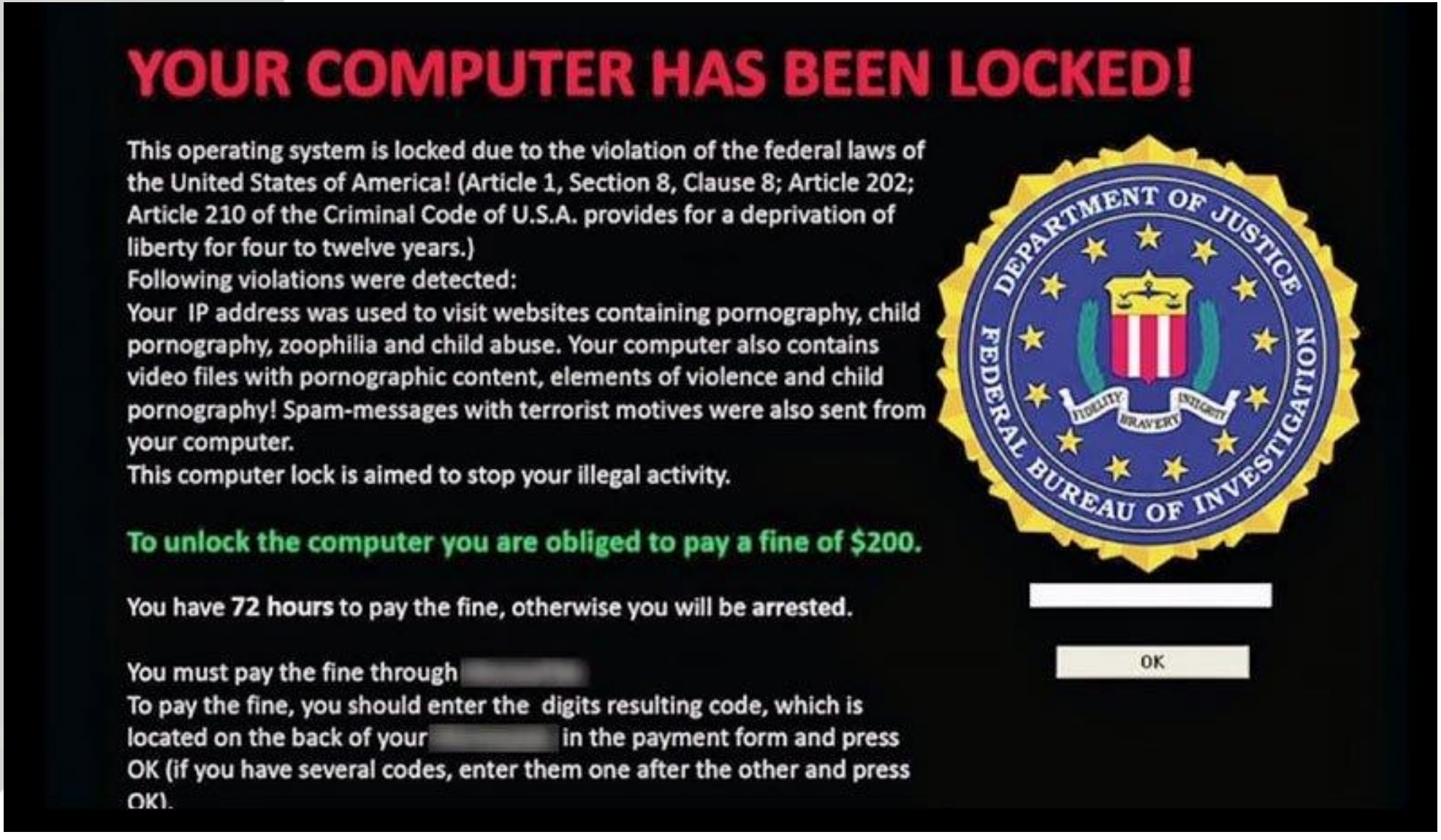
Caso d'uso - ransomware

- **Cos'è un "ransomware"**
  - Malware che minacciano danni se non viene pagato un riscatto

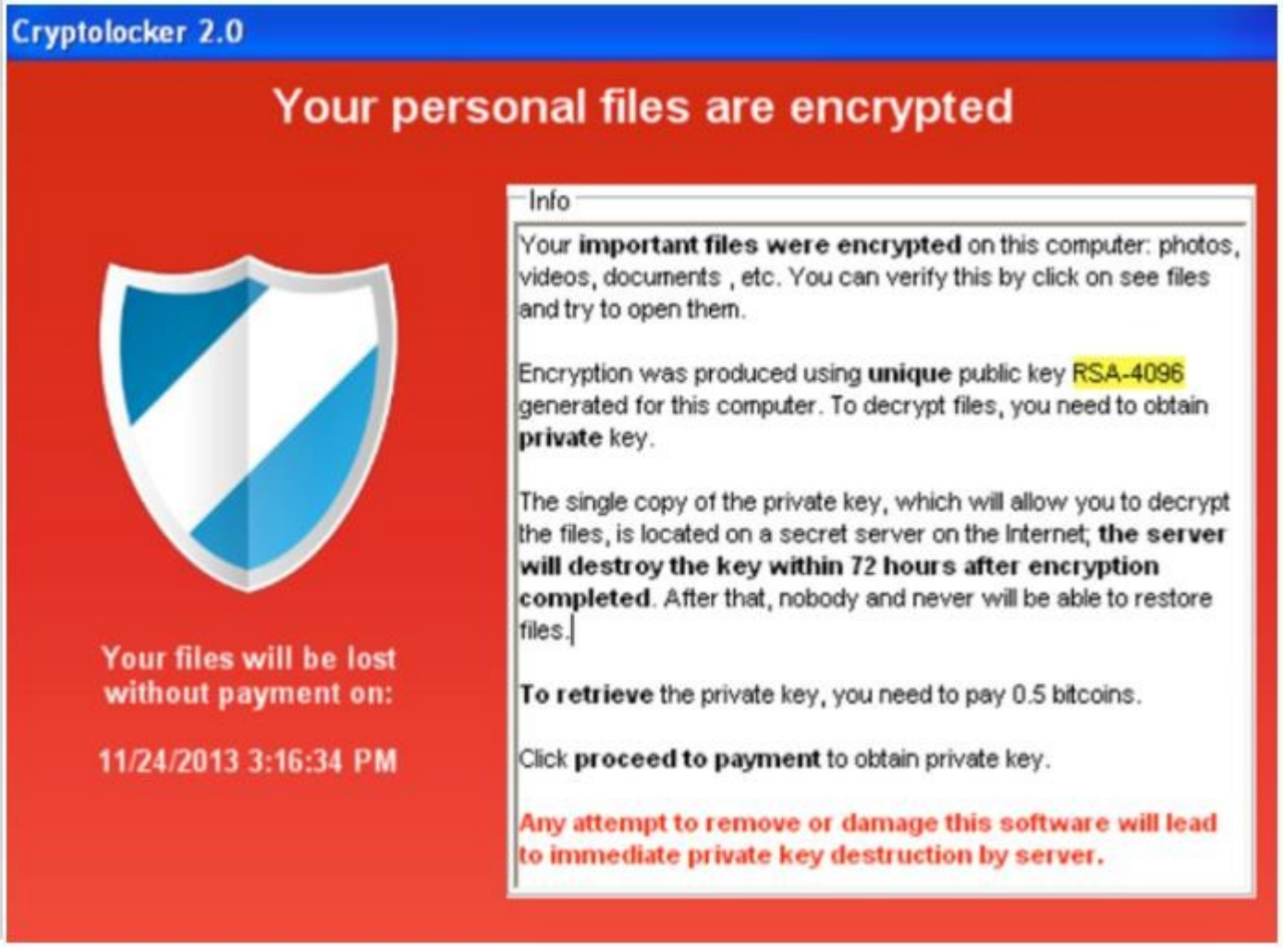
- **Tipi**
  - *Armadietto dello schermo*
  - *File cryptor*
  - *DDOS*
  - *Combinato*

Fonte: Trend Micro

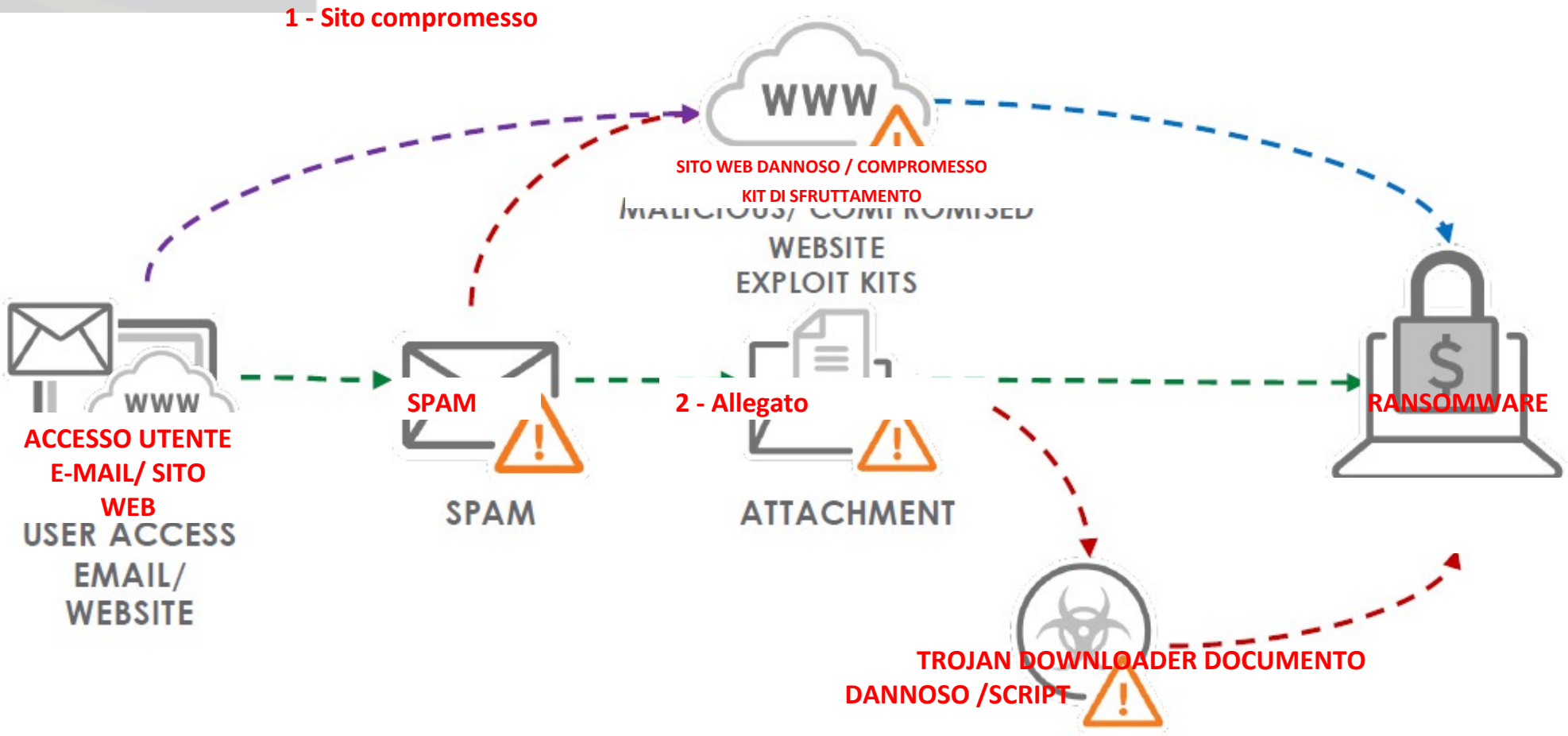
INTRO - Schermo di blocco



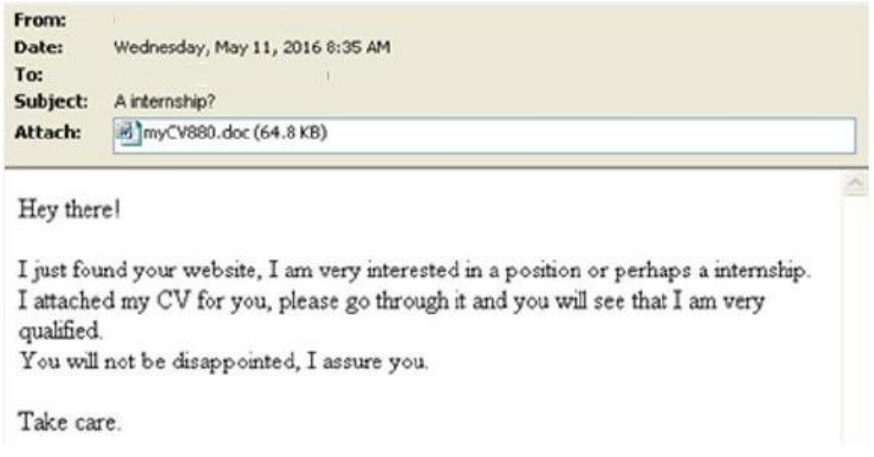
INTRO - Crittografia dei file

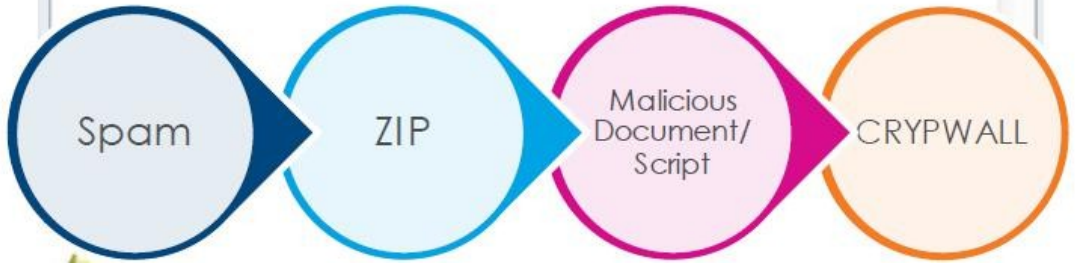


"VETTORE DI ARRIVO "COMUNE



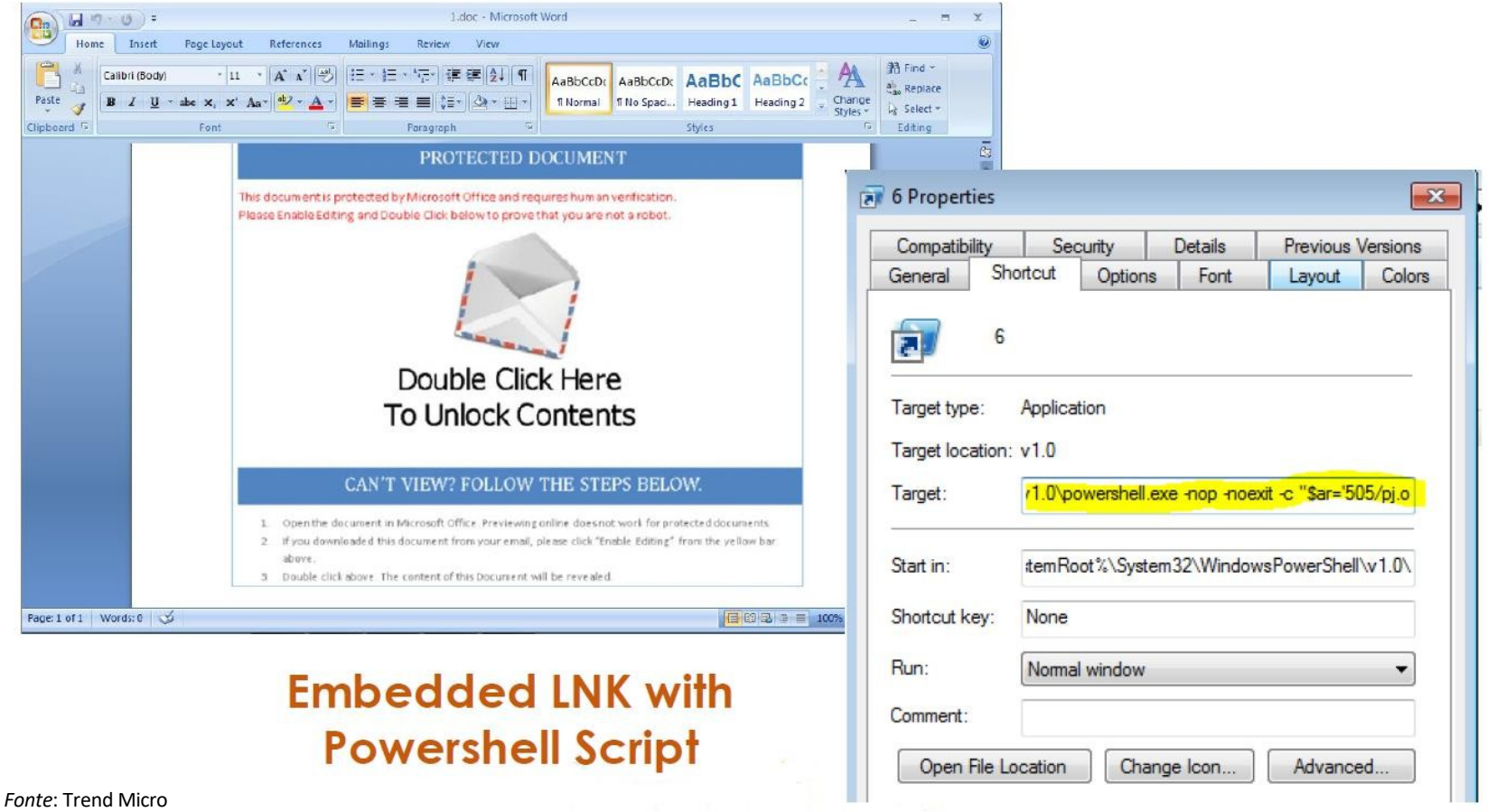
"VETTORE DI ARRIVO "COMUNE





Fonte: Trend Micro

"VETTORE DI ARRIVO "COMUNE



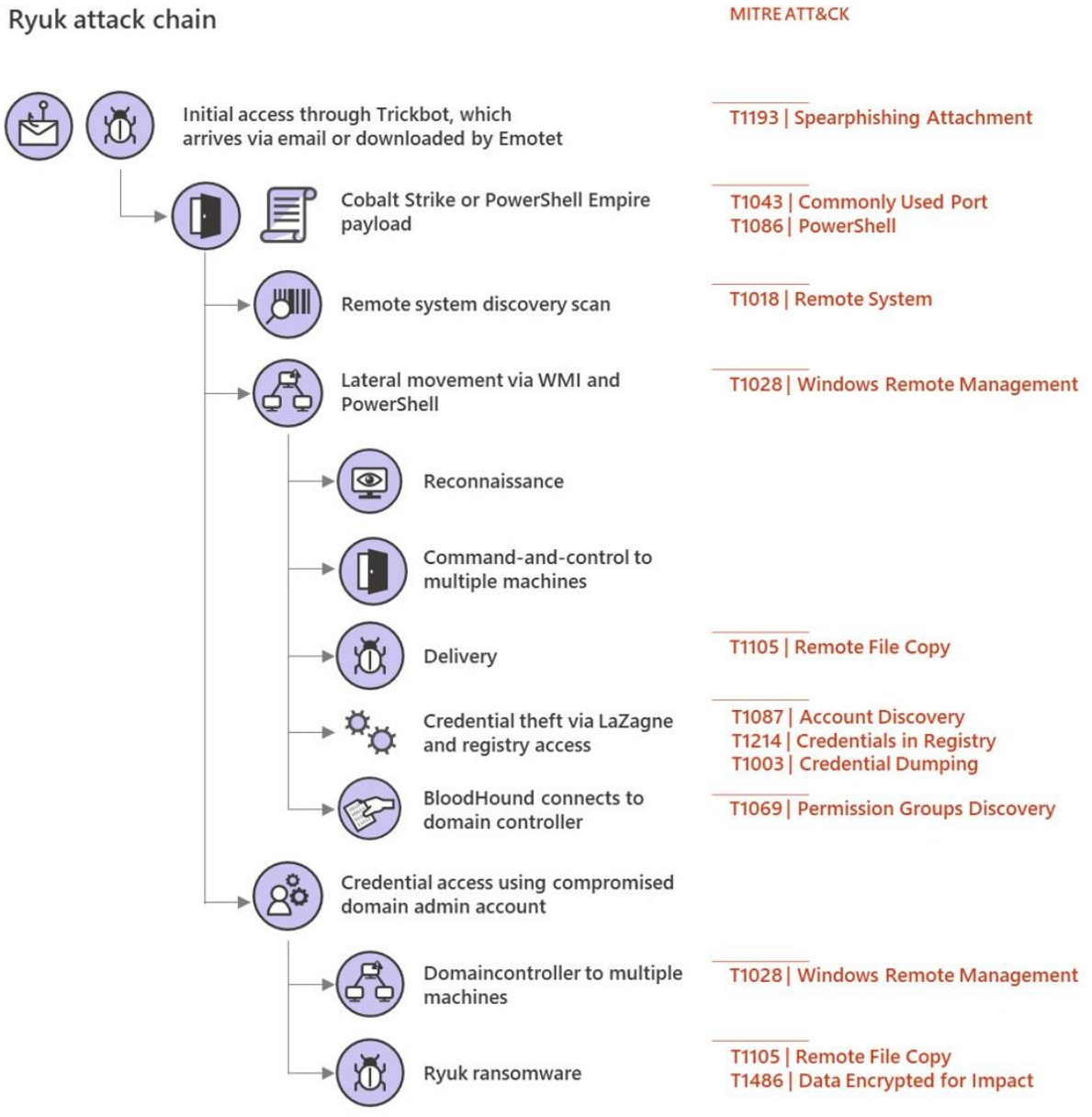
Fonte: Trend Micro

INTRODUZIONE - STORIA

- 1989 - "PC CYBORG"
  - PC bloccato per "licenza scaduta
  - distribuito alla conferenza dell'OMS sull'AIDS (floppy disk)
  - crittografia dei file su disco
- 2005-2006 - prima ondata di ransomware "moderno" (in Russia)
- 2011 - SMS ransomware (comporre un numero SMS premium)
- 2012 - Finto ransomware "Screen Locker" basato sulla polizia
- 2013 - Cryptolocker (crittografia forte, uso di TOR)
- 2014 - La "frenesia" dei file cryptor: CryptoWall, CTB-Locker, Locky, TeslaCrypt …
- 2017 - WannaCry (con funzionalità di "worm")
- 2018 - NotPetya (gomma)
  - colpire la compagnia marittima danese "Maersk" (10 giorni di ferie!)
- 2019 - Labirinto (doppia estorsione)
- 2021 - Tripla estorsione (con l'aggiunta della minaccia DDOS)

NUOVE TENDENZE

- **Ransomware gestito dall'uomo**
  - vettori di infezione personalizzati (ricognizione)
  - scoperta di obiettivi (di alto valore)
  - Escalation dei privilegi - Movimento laterale
  - TTP simile all'APT



TENDENZE "COMUNI"

- **Broker di accesso iniziale (IAB)**
  - Trovare un modo per farsi strada nelle reti di organizzazioni "casuali".
  - Vendere l'accesso alla rete (di solito tramite il dark web, 500-10.000$)
- **RaaS** - Ransomware come servizio
  - malware può essere portato
  - La piattaforma di utilizzo remoto del malware può essere portata
    - Configurazione: tassa di riscatto, nota di pagamento, vittime...
  - la piattaforma può già fornire l'accesso alle vittime
    - Ad esempio Emotet (downloader generico)

Argomento 2 - Minacce

Settore marittimo

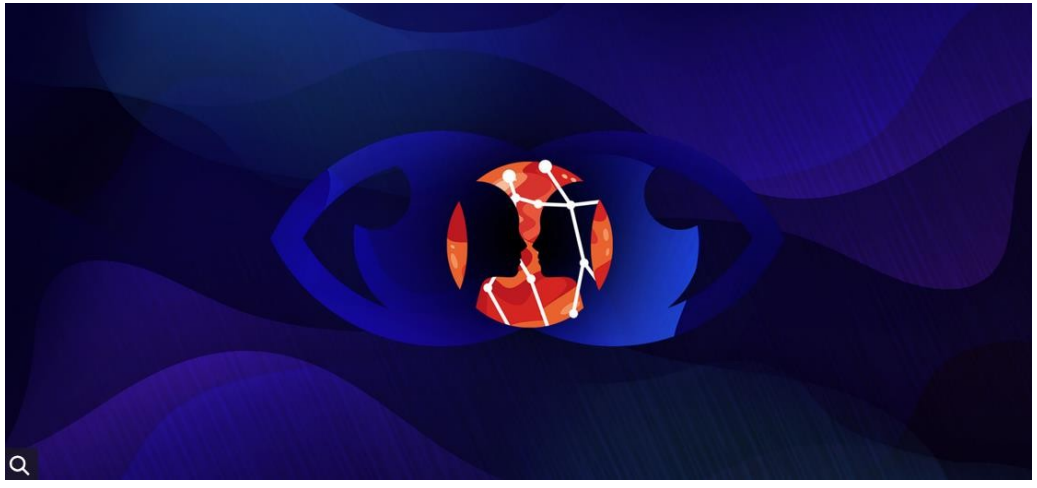
- Fonti identificate
- Casi d'uso

Fonti di intelligence (aziende)

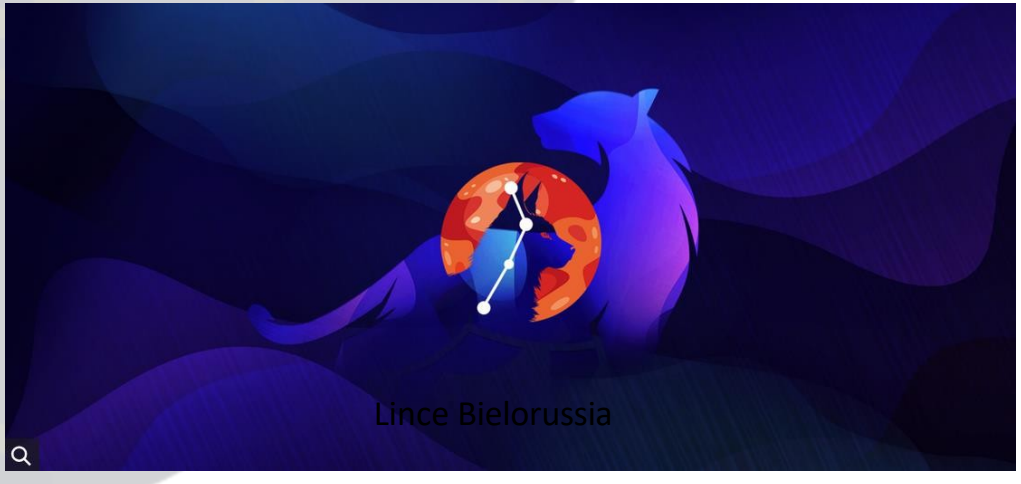
Gruppi di attori pericolosi monitorati dall'unità 42 di Palo Alto Networks

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

Draco PAKISTAN



Gemini INDIA



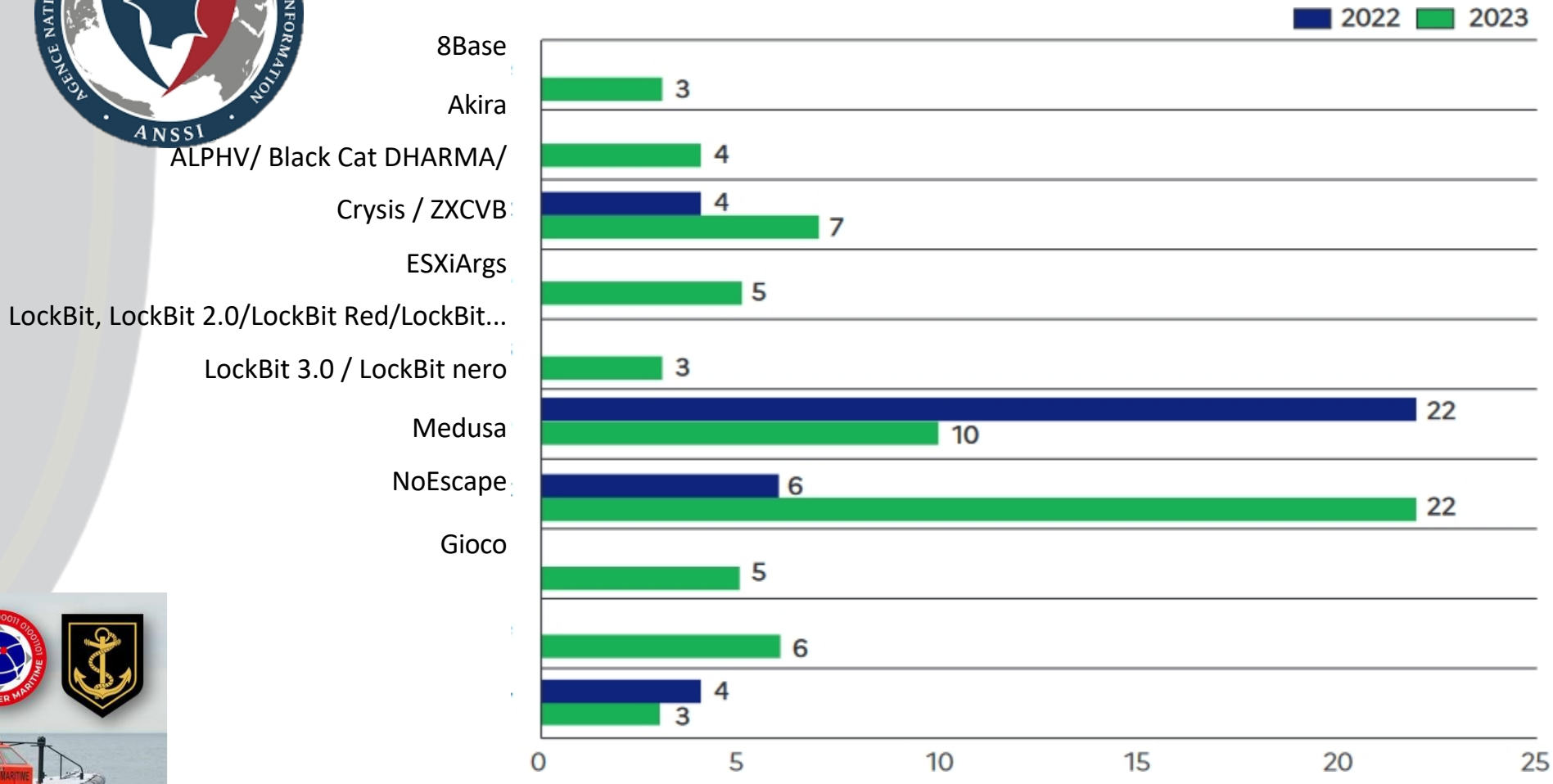
Lince Bielorussia

Problema: la posizione giuridica degli attori Rogue

RaaS: RANSOM come servizio

Fonti di intelligence (Agenzie nazionali)

Confronto tra i principali ceppi di ransomware utilizzati negli incidenti segnalati all'ANSSI nel 2022 e nel 2023



RANSOMWARE nel dominio marittimo

- **Tendenze**
  - crescente digitalizzazione
  - naturale passaggio da operazioni condotte localmente a operazioni remote
  - COVID-19 boost remoto
- **Attacchi ransomware: aspetti peculiari?**
  - stessi aggressori, stessi TTP
  - obiettivo interessante: supporta il 90% del commercio mondiale!
    - potenziale obiettivo di guerra
  - ecosistemi IT complessi e integrati (anche con l'Operation Technology - OT)
    - rischi di aumento della catena di fornitura: il "punto di ingresso" può essere un'azienda partner!
    - molti vettori di attacco disponibili per gli aggressori
  - Le spedizioni sono un punto chiave della catena logistica.
    - può essere utilizzato come passo intermedio per raggiungere altri obiettivi (attacco alla catena di approvvigionamento).

RANSOMWARE nel dominio marittimo

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.

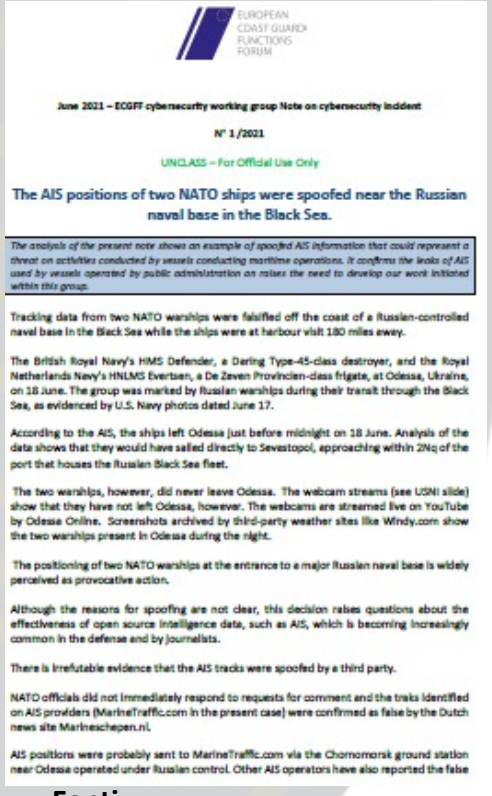
Soluzioni

- **Implementa le migliori pratiche di sicurezza informatica**
- **Principali temi di mitigazione**
  - **autenticazione forte** (soprattutto per portali e VPN rivolti a Internet)
    - o **approccio a fiducia zero**, in un approccio senza perimetro
  - **principio del minimo privilegio** (soprattutto con i privilegi degli utenti)
  - **segregazione di rete (logica fisica)**
  - Procedure di **continuità aziendale**
    - **backup** (caldo e freddo)
  - **Valutazione** continua **delle vulnerabilità** e **patch**
  - Monitoraggio **del Centro operativo di sicurezza**
  - **Hardening (**protocolli di rete, firewall host, configurazione software, sicurezza del sistema operativo, …)

Caso d'uso - AIS / GNSS

Principale preoccupazione per le agenzie marittime - Spoofing AIS / GNSS / Jamming

Le posizioni AIS di due navi della NATO sono state sottoposte a spoofing nei pressi della base navale russa nel Mar Nero.



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 Dering 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

Fonti:

- CERTIFICATO UE E CERTIFICATO M
- Stati membri
- Aziende private

Minacce alle infrastrutture critiche

Malware:
Malware la cui diffusione è incontrollabile

Script kiddy (adolescente inattivo o, più in generale, attaccante solitario e opportunista):

- Mezzi molto bassi (€<.100)
- Gioco d'azzardo (e possibilmente profitto) come motivazione

Attacco opportunistico Dipendente malintenzionato (rancore/ragione):

- Mezzi bassi (< 1.000 euro)
- Motivazione principale: danneggiare il proprio datore di lavoro, evitare le vittime
- Discrezione quando possibile
- Facile accesso a tutti gli elementi dell'imbarcazione

Gruppo terroristico:

- Mezzi moderati (da 10.000 a 50.000 euro)
- Ricerca di vittime umane, danni materiali, alta visibilità mediatica

Impresa criminale:

- Risorse elevate (circa un milione di euro)
- Obiettivo di redditività
- Bassi vincoli morali
- Cerca la discrezione

Stato:

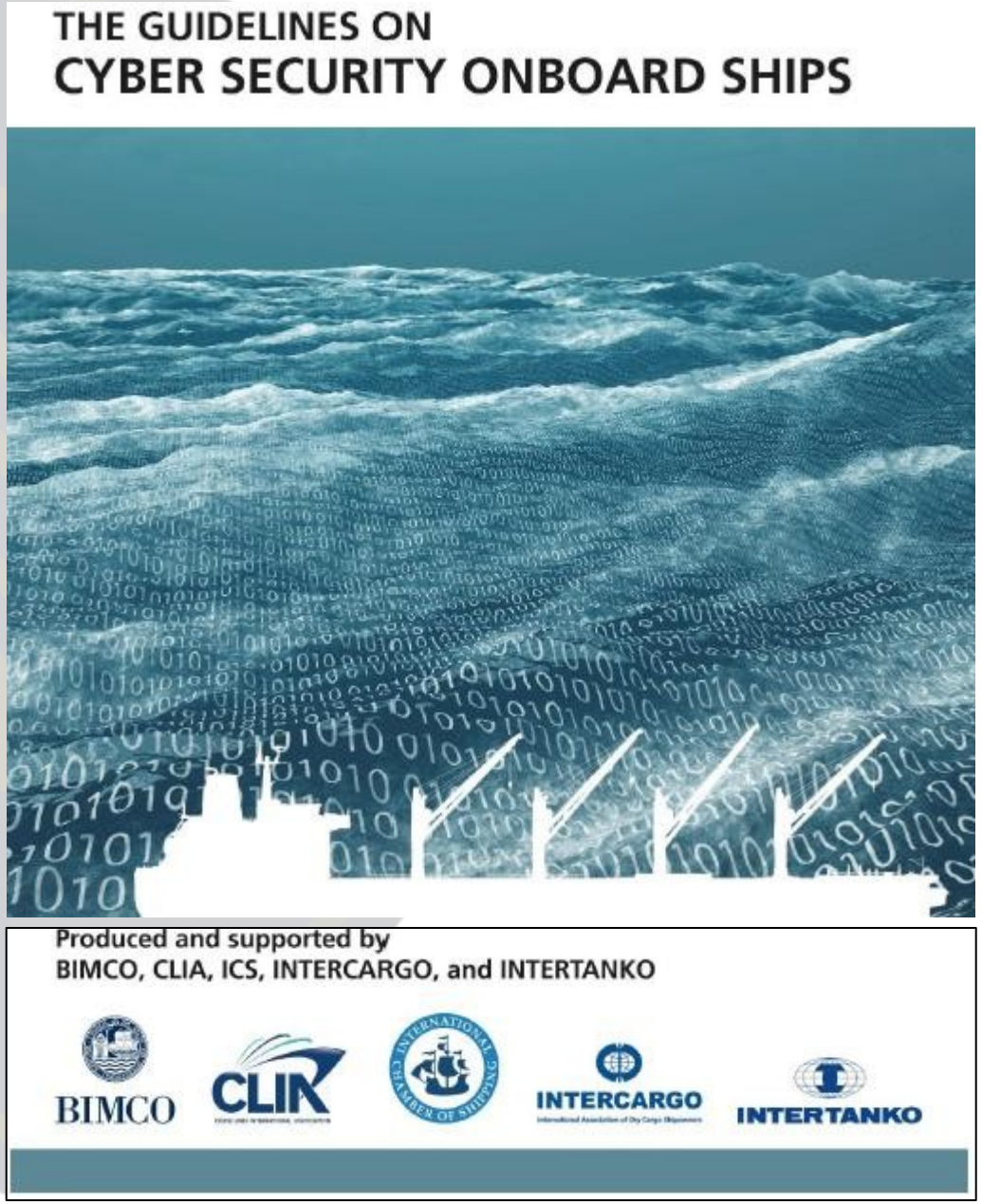
- Mezzi quasi illimitati
- Obiettivi di tutti i tipi -
- Assenza di vincoli morali
- Discrezione necessaria

Minacce ai sistemi

Spoofing della nave - Viene trasmesso un messaggio AIS che fornisce i dettagli di una nave inesistente. Gli scenari in cui questo potrebbe essere utilizzato includono lo spoofing di una nave di una nazione nelle acque territoriali di una nazione ostile, inducendo quest'ultima a prendere contromisure. In alternativa, è possibile trasmettere versioni multiple dei dettagli di una nave reale, posizionandola contemporaneamente in molti luoghi diversi per oscurare la sua vera posizione (ad esempio, per la pesca illegale).
spoofing degli aiuti alla navigazione - Vengono trasmessi falsi aiuti alla navigazione, come ad esempio una boa che avverte della presenza di secche nascoste, per costringere una nave a cambiare rotta. Questo potrebbe essere fatto per costringere una nave a entrare in una zona in cui può essere dirottata.
Spoofing delle collisioni - La prevenzione delle collisioni è uno degli usi principali dell'AIS. Fornendo dettagli spoofati di un'imbarcazione in rotta di collisione, un aggressore può costringere la nave a cambiare rotta per evitare la collisione prevista. Questo potrebbe, esempio, essere utilizzato per guidare la nave verso una vera e propria collisione.

Spoofing AIS-SART - La ricerca e il soccorso sono un altro degli usi principali dell'AIS. Questo attacco genera un segnale spoofing del transponder SAR-T, che fornisce i dettagli di una richiesta di soccorso. Poiché le navi sono legalmente obbligate a prestare soccorso, lo spoofing SART può essere utilizzato come esca per attirare le imbarcazioni in una posizione in cui possono essere attaccate.
Spoofing delle previsioni meteorologiche - L'AIS può essere utilizzato per trasmettere informazioni sulle condizioni meteorologiche prevalenti tra le imbarcazioni. Una previsione falsa, in particolare quella che prevede condizioni ottimali quando è in arrivo una tempesta, potrebbe essere utilizzata per mettere in difficoltà le imbarcazioni.
Dirottamento AIS - È anche possibile annullare i segnali inviati dalle imbarcazionitrasmettendo un segnale di potenza superiore alla stessa ora e frequenza. L'aggressore può quindi modificare alcuni dettagli messaggio originale, ad esempio suggerendo che l'imbarcazione ha un carico nucleare in una zona in cui tale carico è illegale.

Responsabilità condivise - Grande comunità - Iniziative limitate



- Paesi di bandiera
- Armatori
- Società di gestione navale
- Porti
- Connettori all'economia (regionale, trasporti)
- Agenti marittimi
- Compagnie di assicurazione
- Agenzie di certificazione
- Costruttori navali
- Operatori COMMS
- Fornitori di sistemi
- Fornitori di sicurezza

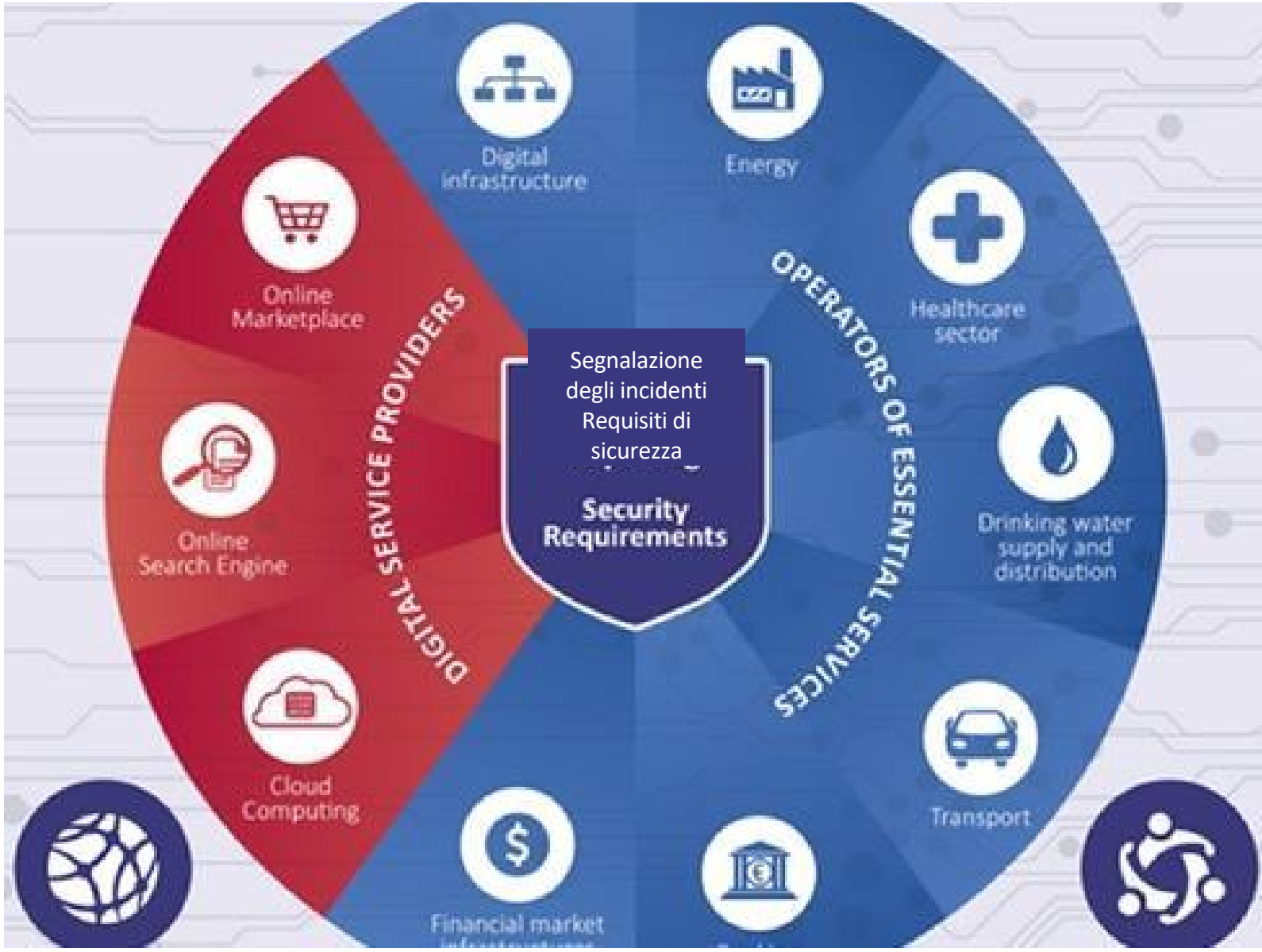
Condizioni di utilizzo

I consigli e le informazioni fornite nelle Linee guida sulla sicurezza informatica a bordo delle navi sono da intendersi come puramente orientativi **e devono essere utilizzati a rischio e pericolo dell'utente**. *Gli Autori, i loro membri o i dipendenti di qualsiasi persona, azienda, società o organizzazione non forniscono alcuna garanzia o dichiarazione, né accettano alcun obbligo di diligenza o responsabilità ... per l'accuratezza delle informazioni o dei consigli forniti nelle Linee guida o per qualsiasi omissione nelle Linee guida o per qualsiasi conseguenza derivante direttamente o indirettamente dall'osservanza, dall'adozione o dall'affidamento sulle indicazioni contenute nelle Linee guida, anche se causata da un mancato esercizio di ragionevole diligenza da parte di una delle suddette parti.*

Minacce / Impatti

Specificità marittime

- Comunità
- Somiglianza Marittimo/Digitale
- Dipendenza dal GNSS
- Ambiente di condivisione delle informazioni



Rischi delle infrastrutture critiche marittime

Argomento 3 - L'importanza dei dati

- Regolamento UE
- Dati classificati / Dati sensibili
- Trattamento dei dati

Analogie marittime/digitali

	Marittimo	Digitale
Dimensione	80% della terra	Illimitato
Legale	Debolezza della regolamentazione internazionale UNCLOS	Regolamentazione internazionale limitata GDPR
Economico	90 % del commercio internazionale Stabile	50 % delle transazioni internazionali Crescita permanente
Ambiente	Imprevedibile: Stato del mare, vento, salsedine, pericoli fisici	Imprevedibile: Virtualità,
Minaccia	Attività e manipolazioni illegali, Pirateria, terrorismo	Portata globale delle minacce informatiche Attività illegali incentrate sui beni
Focus	Informazioni sulle azioni IFC) Capacità di agire = Stati	Prevenzione e condivisione delle informazioni Coordinare l'azione

Marittimo e digitale: somiglianze

Mondi simili (stesse valutazioni - stesse conseguenze?)

800 - 1260 T rubino

In 10 secondi....

225.000 GB di dati

- 500.000 messaggi Facebook,
- 57.000 tweet,
- 46.000 ricerche su Google
- 2 milioni di messaggi su WhatsAp

Piano di comunicazione

Adattato agli operatori

Infrastrutture critiche

Direttiva ECI 2008

Rischio globale (sicurezza, espionnage, dati, attività)

L'attacco potrebbe mettere in pericolo la sicurezza di un paese

Monitoraggio settoriale

- Analisi del rischio
- Vulnerabilità
- Direttive

Coordinamento intersettoriale

Operatore del servizio essenziale

Direttiva NIS 2015

Rischio di espionnage, dati, attività

L'attacco potrebbe mettere in pericolo l'attività economica

Valutazione del rischio settoriale

Avvertenze

Informazioni intersettoriali

Utente comune del dominio Maritim

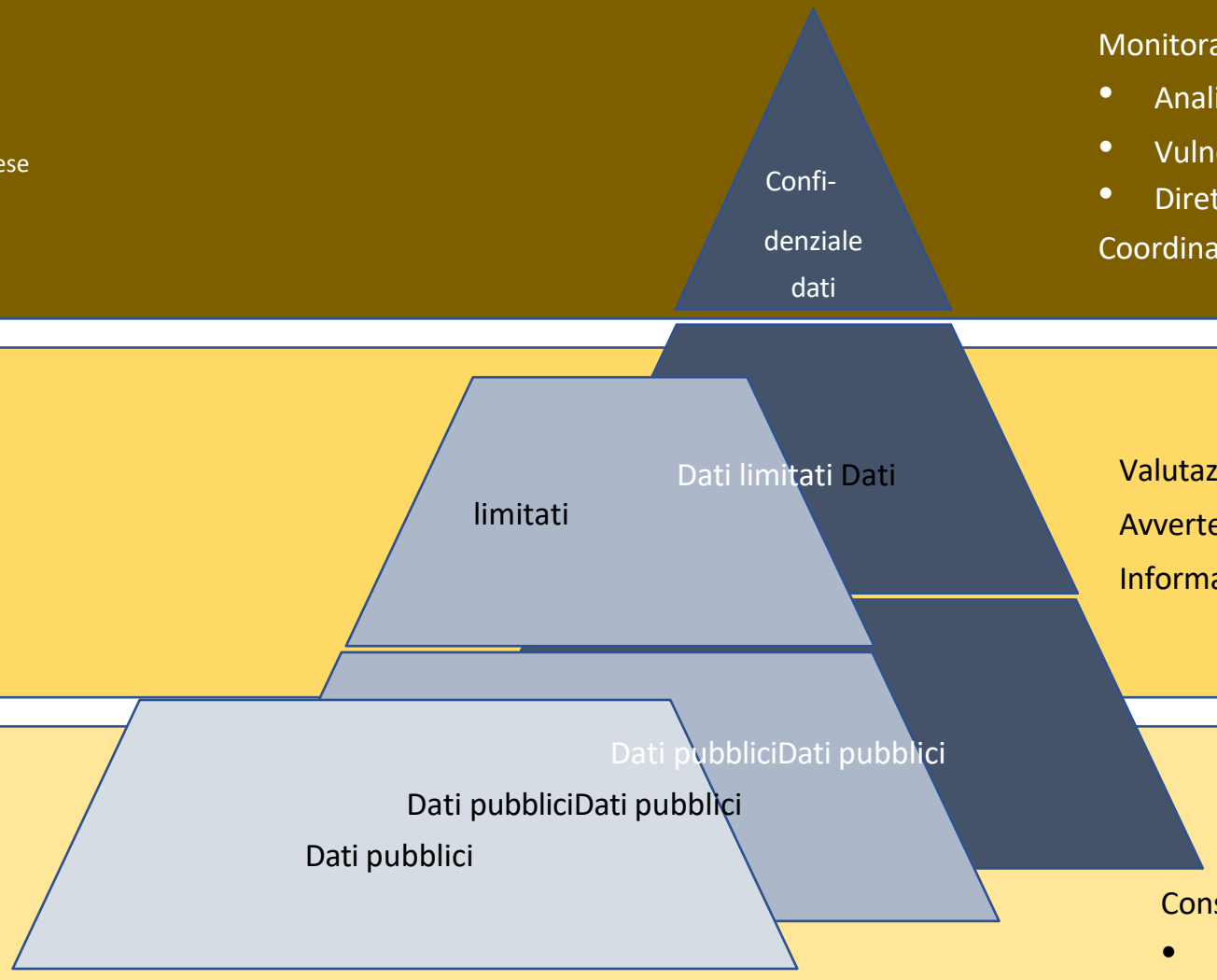
GDPR 2018

Rischio per i dati

L'attacco potrebbe rappresentare una minaccia

Consapevolezza settoriale

- Raccomandazioni
- Prevenzione



QUADRO EUROPEO DELLE COMPETENZE DI CYBERSECURITY: PROFILI PROFESSIONALI

European Cybersecurity Skills Framework (ECSF)

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

https://cybersecpro-project.eu/

Caso d'uso

Infrastrutture critiche

Porto marittimo

PORTI E PARTI INTERESSATE DEL SETTORE MARITTIMO

Quale obiettivo per gli attaccanti?

Sicurezza delle informazioni

Aree funzionali

(Tassonomia CYBERSECPRO)

Privacy e protezione dei dati

Gestione del rischio di sicurezza informatica

Minaccia alla sicurezza informatica

gestione

Incidente informatico

Risposta

Aspetto umano della sicurezza informatica

Test di penetrazione

Sicurezza delle reti e delle comunicazioni

Strumenti e tecnologia

Gestione della sicurezza informatica

Politica, processo e conformità della sicurezza informatica

Quadro marittimo - Legale (internazionale) RISOLUZIONI

DELL'IMO

MSC.428(98) (16 giugno 2017) MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS:
un sistema di gestione della sicurezza approvato deve tenere conto della gestione del rischio informatico

Le amministrazioni dovrebbero garantire che cyber rischi informatici sono adeguatamente affrontati in sicurezza
sistemi di gestione 01 gennaio 2021 (indagine ?)

Sistemi particolari da considerare:

- Sistemi a ponte
- Sistemi di movimentazione e gestione dei carichi
- Sistemi di gestione della propulsione e dei macchinari e sistemi di controllo della potenza
- Sistemi di controllo degli accessi
- Sistemi di assistenza e gestione dei passeggeri
- Reti pubbliche rivolte ai passeggeri
- Sistemi amministrativi e di welfare per l'equipaggio
- Sistemi di comunicazione

Incident notification requirements
- Specific criteria/thresholds for incident notification

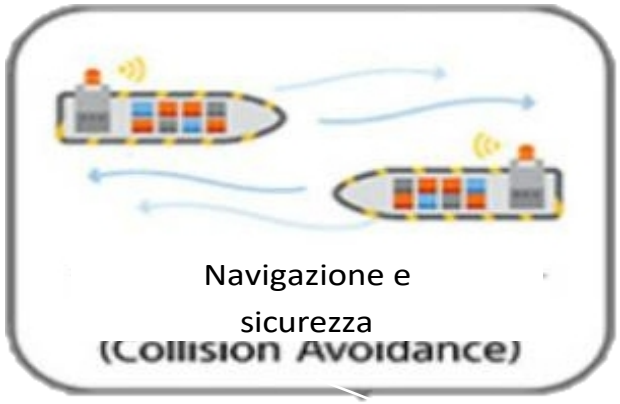
Quadro marittimo - Legale (UE) - Promemoria

	Riferimento	Utente	Netto	SI	Chi è interessato	Misure preventive	Capacità di difesa	Riconquista (giudiziaria)
C I (Nazioni: dopo il 2013) 	Direttiva 2005/65/CE Normativa nazionale	+++	++	++ +	Porti Cable Oil & gaz HAZMAT e i loro sistemi critici	L'UE ha identificato i porti come elementi critici infrastruttura" Porto = area specifica di terra e acqua, con confini definiti dallo Stato membro, contenente opere e attrezzature destinate a facilitare le operazioni di trasporto.	Registrazione degli eventi e capacità di analisi dei registri Sonde ai sistemi (Stato o fornitore di servizi qualificato. ANSSI permalink Gestione delle crisi	Conservazione della documentazione tecnica per 6 mesi
OES (NIS - 2018 - 22) 	Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio (6/07/16). - misure per garantire un livello di sicurezza di sistemi e reti	0	+++	++	Elenco **OES** fornito dalle Nazioni (porti, compagnie marittime)	Elenco dei servizi essenziali Governance politica e tecnica. Protezione della rete e dell'IS. Controlli decisionali PM, standard Regole dei fornitori cloud	Difesa delle reti e dei sistemi informativi; Utilizzo di dispositivi hardware/software o servizi IT certificati per la sicurezza. Segnalazione di incidenti all'Agenzia nazionale per la sicurezza.	Resilienza aziendale.
Dati (GDPR-2018) 	Regolamento UE 2016/679 - 27/04/16 dati - protezione delle persone fisiche Regolamento	+++	0	++	Soggetto che gestisce i dati personali (Agente di trasporto traghetti)	Protezione delle libertà fondamentali nel mondo digitale (cancellazione e portabilità dei dati).	Sistemi e reti protetti a livello tale da impedire la perdita di controllo delle informazioni personali.	Possibile ricorso ai CERT in caso di perdita/perdita di dati.

Sistemi di controllo portuale (PCS)

Operazioni portuali

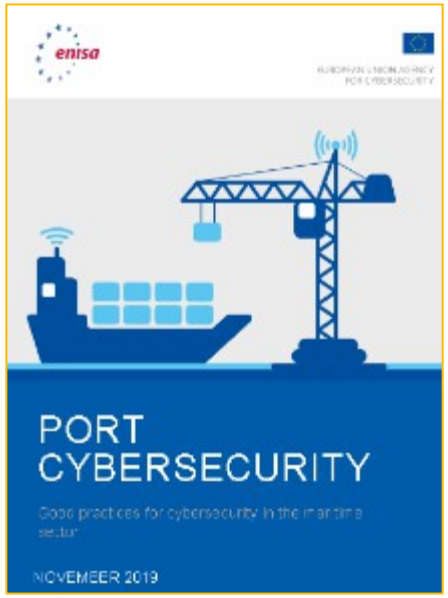
Quali sistemi?

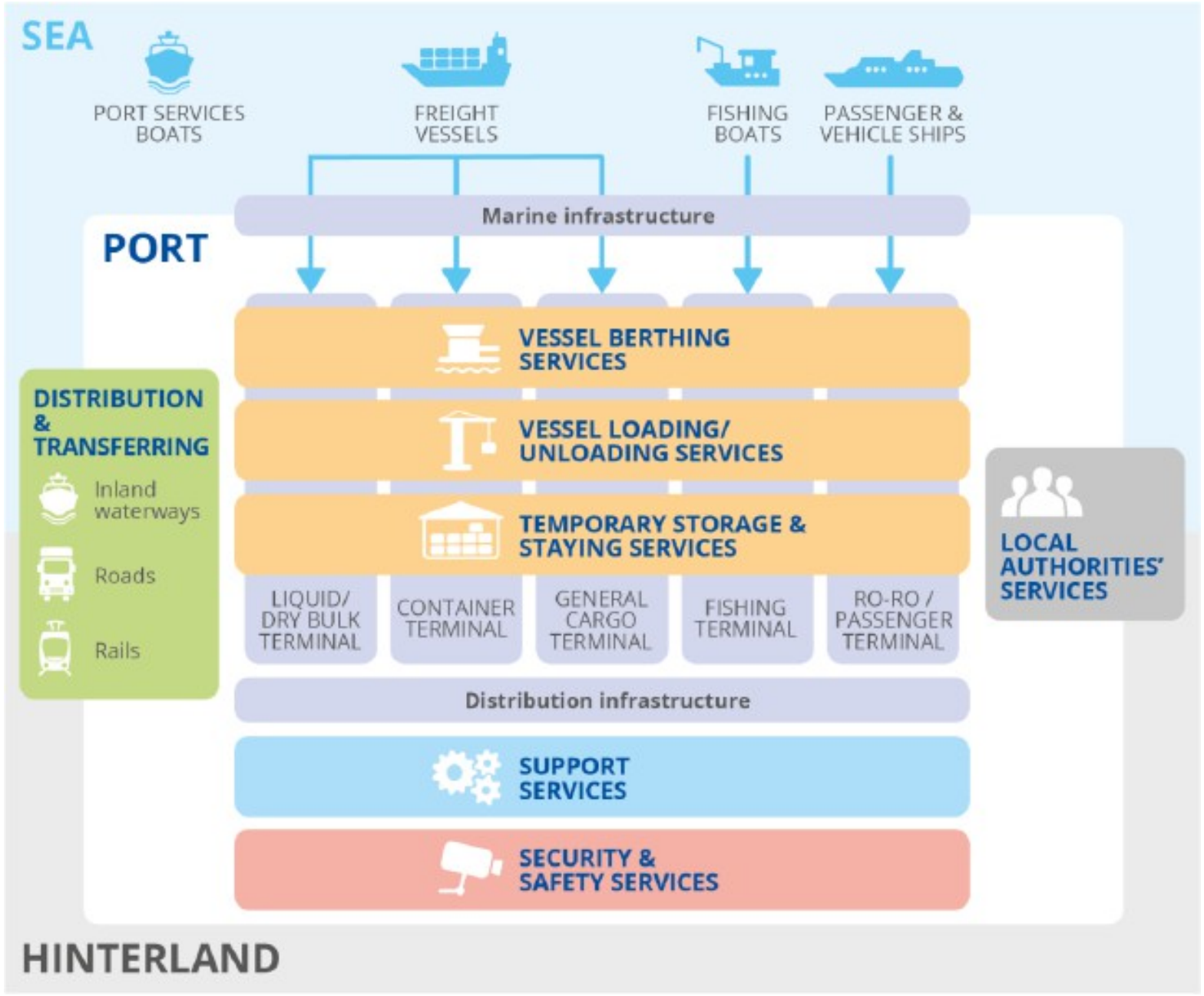


Quadro marittimo - Tecnico

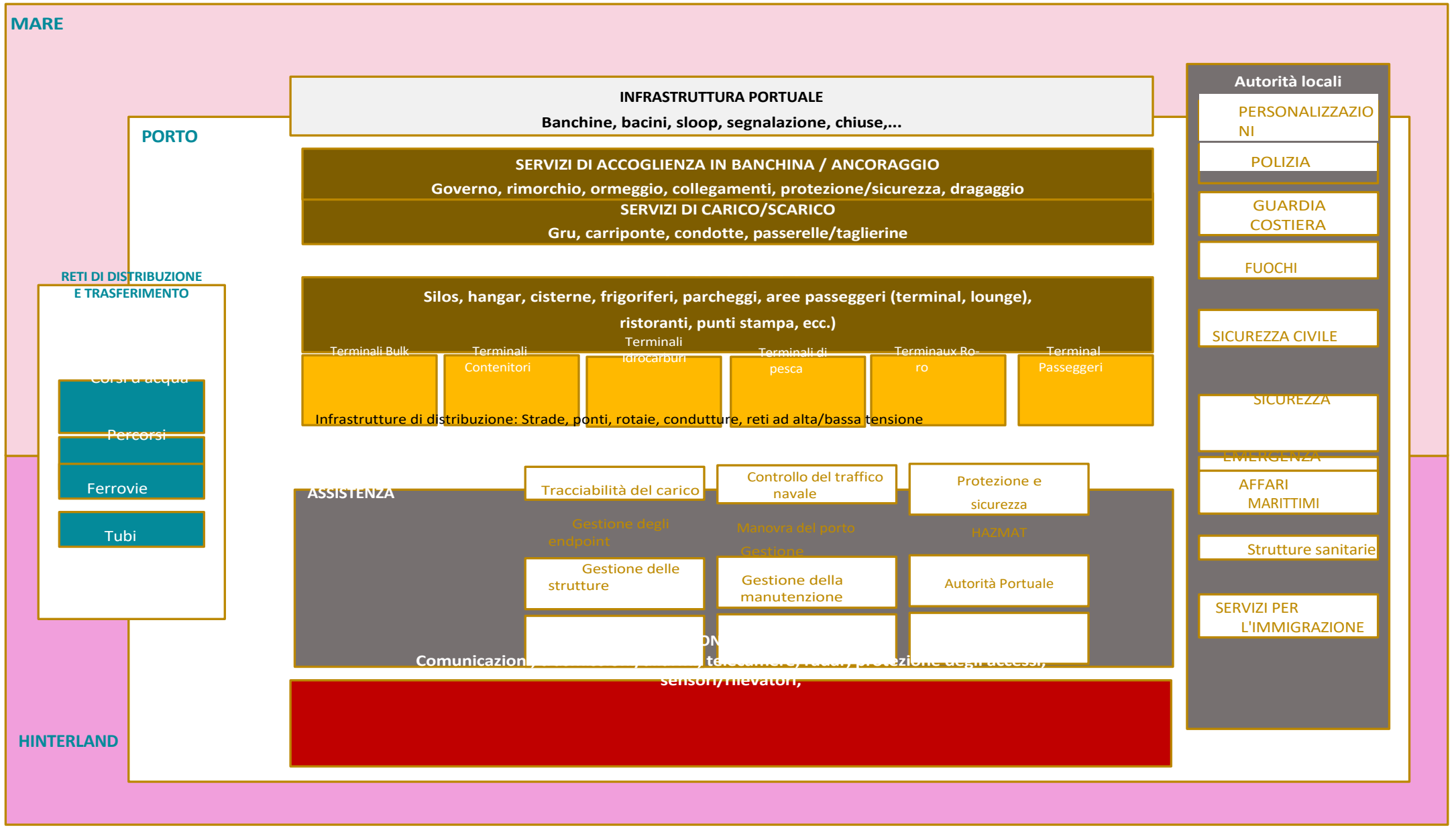
Porto digitalizzato

Cartografia

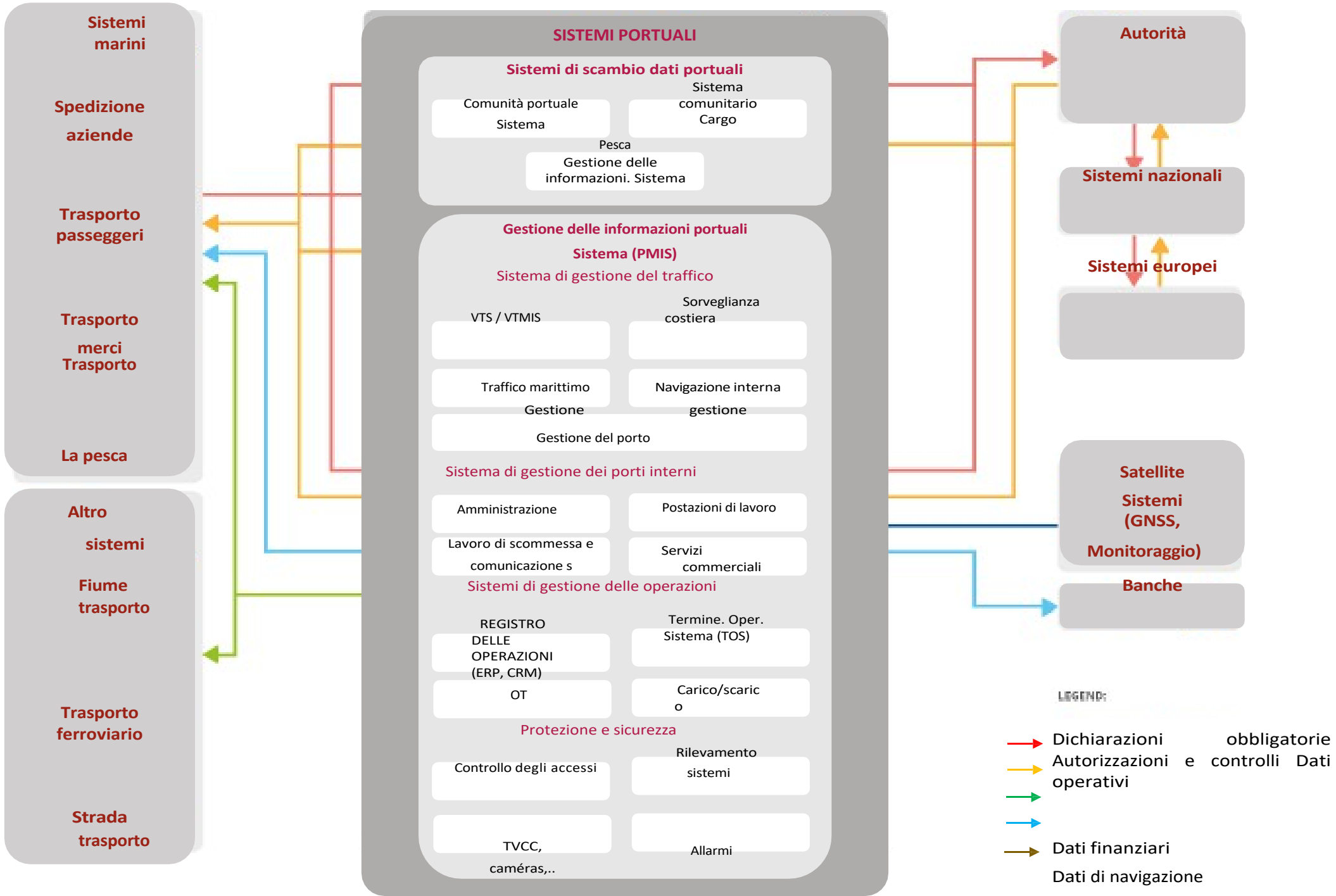




Quadro marittimo - Infrastruttura portuale



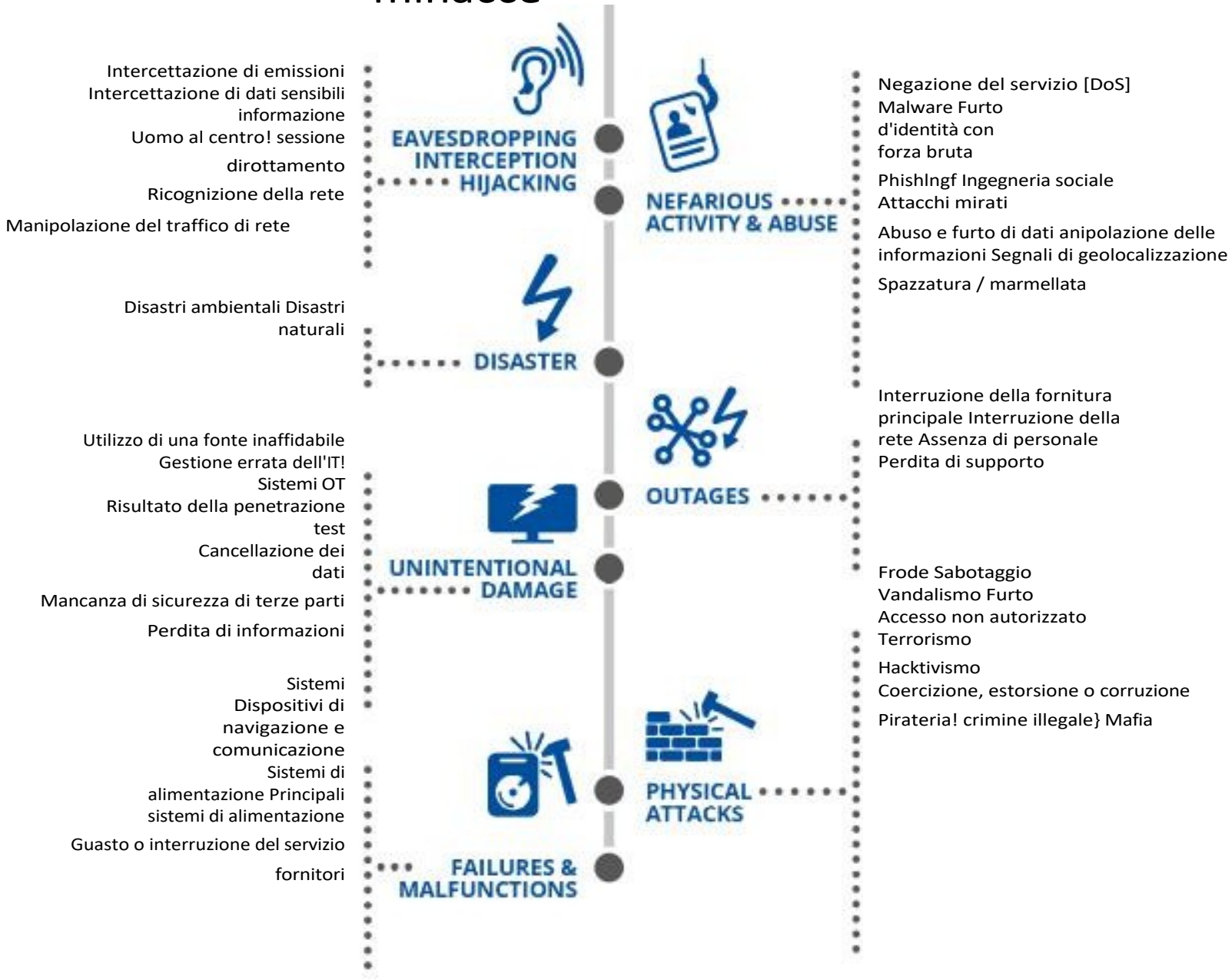
Sistemi portuali



Minacce

Minacce nel settore marittimo

Tassonomia delle minacce

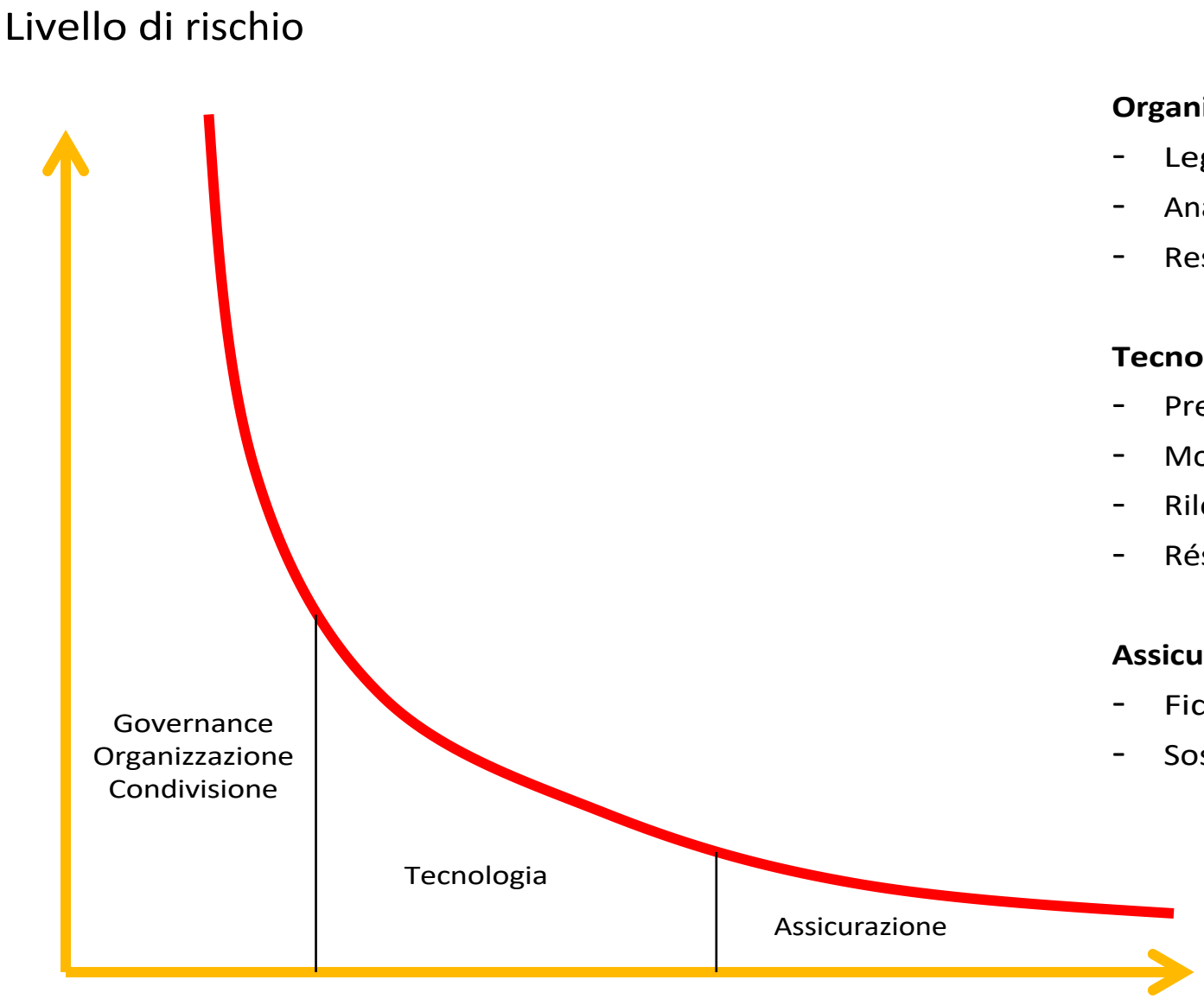


Mitigazioni dei rischi per le infrastrutture critiche

Marittimo

PORTI E PARTI INTERESSATE DEL SETTORE MARITTIMO

Strategie ed effetti della riduzione del rischio di cybersecurity



Organizzazione

- Legge / Governance
- Analisi del rischio
- Resilienza funzionale/settoriale

Tecnologico

- Prevenzione
- Monitoraggio / sorveglianza
- Rilevamento e condivisione degli incidenti
- Résilience

Assicurazione

- Fiducia
- Sostegno finanziario / ricostruzione

DOMANDE?

- BREAK