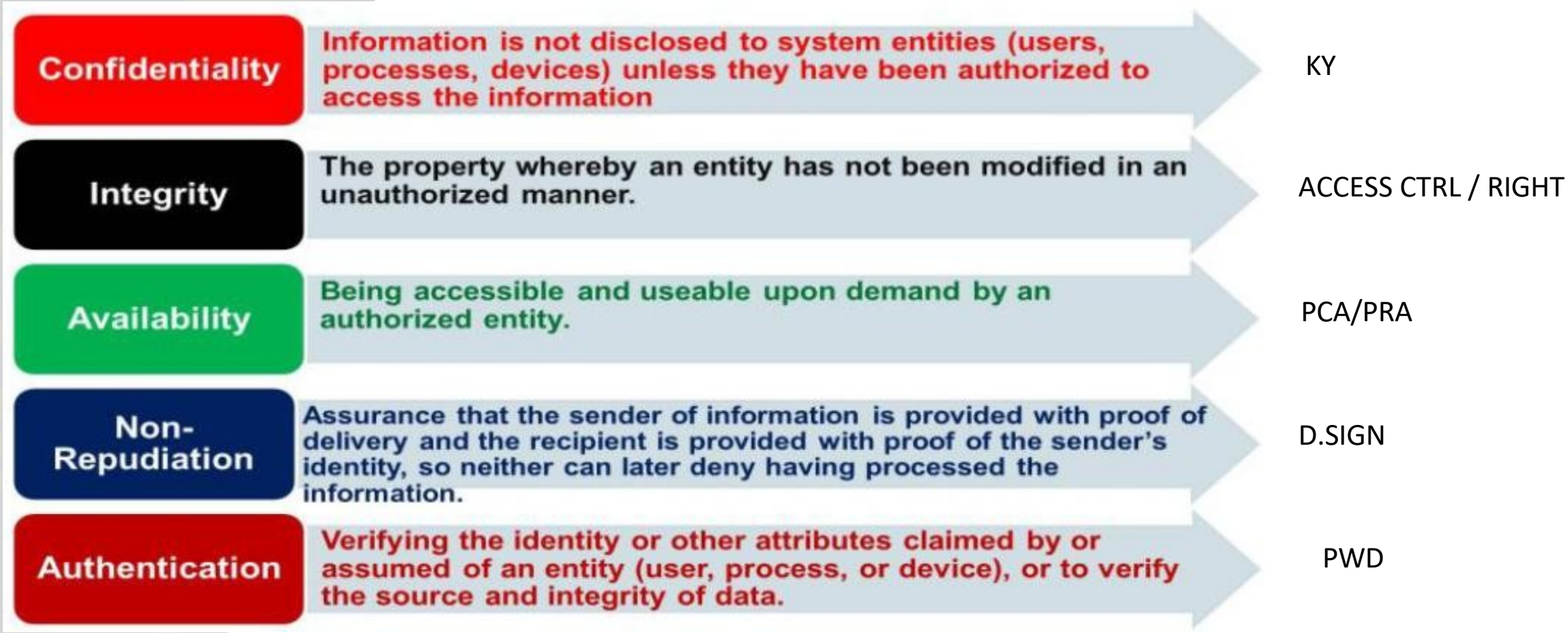
Definizioni dei concetti di sicurezza e protezione

UE7- e C1 Identificare i settori funzionali, mapparli, garantirne un'interoperabilità sicura - Esigenze, constatazioni, analisi

Aree funzionali Interoperabilità

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	Cybersecurity: 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 con collaboratori, fornitori e clienti				

Assicurazione delle informazioni



Aree funzionali

Servizi
Servizi di sicurezza informatica

Tecnico
Soluzioni tecniche

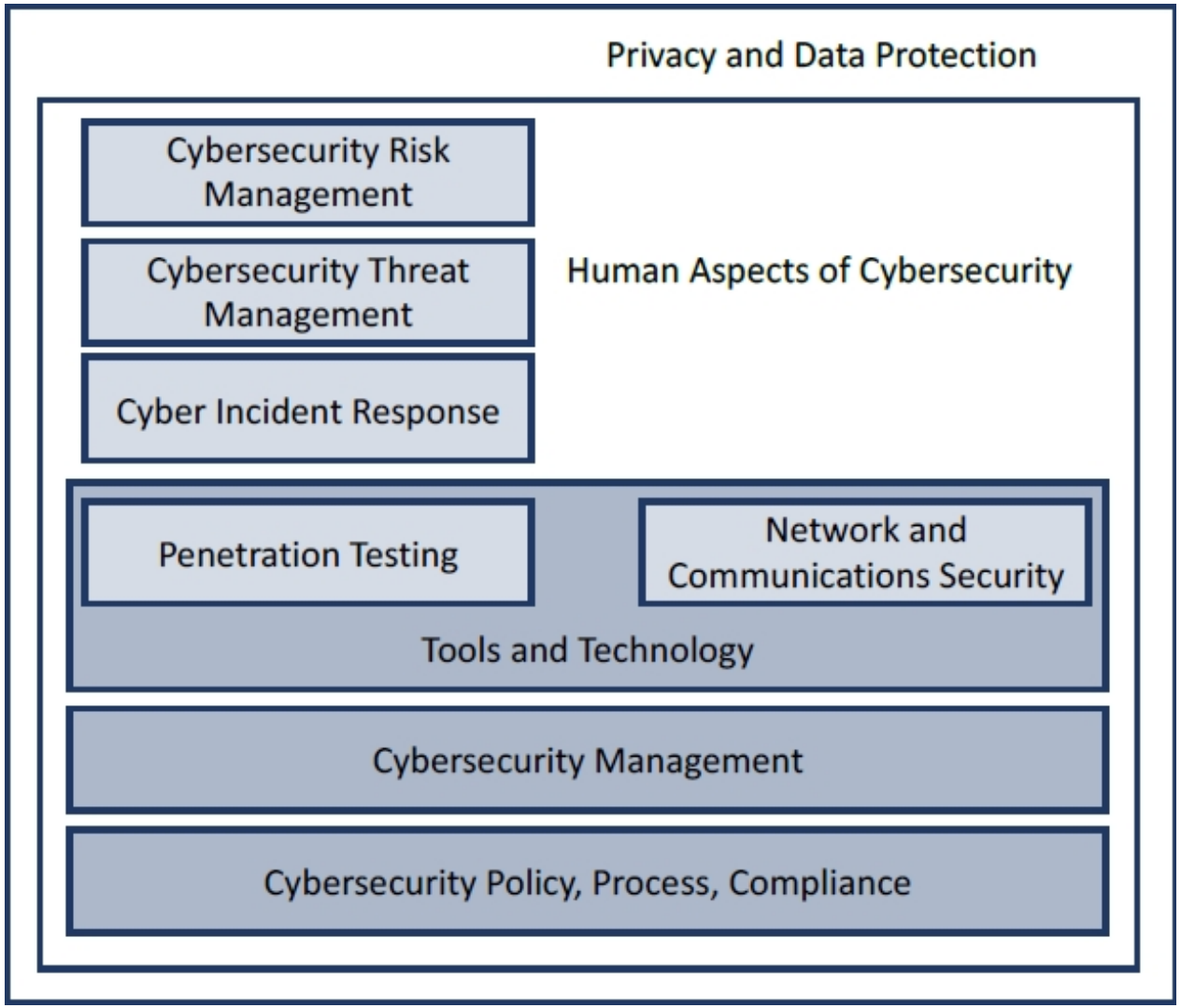
Organizzative
Governance tra enti pubblici e privati

Semantica
Standard e riferimenti comuni

Legal
Leggi e regolamenti internazionali / cooperazione tra magistratura e forze dell'ordine

Aree funzionali – Cyber

(Visione CYBERSECPRO)

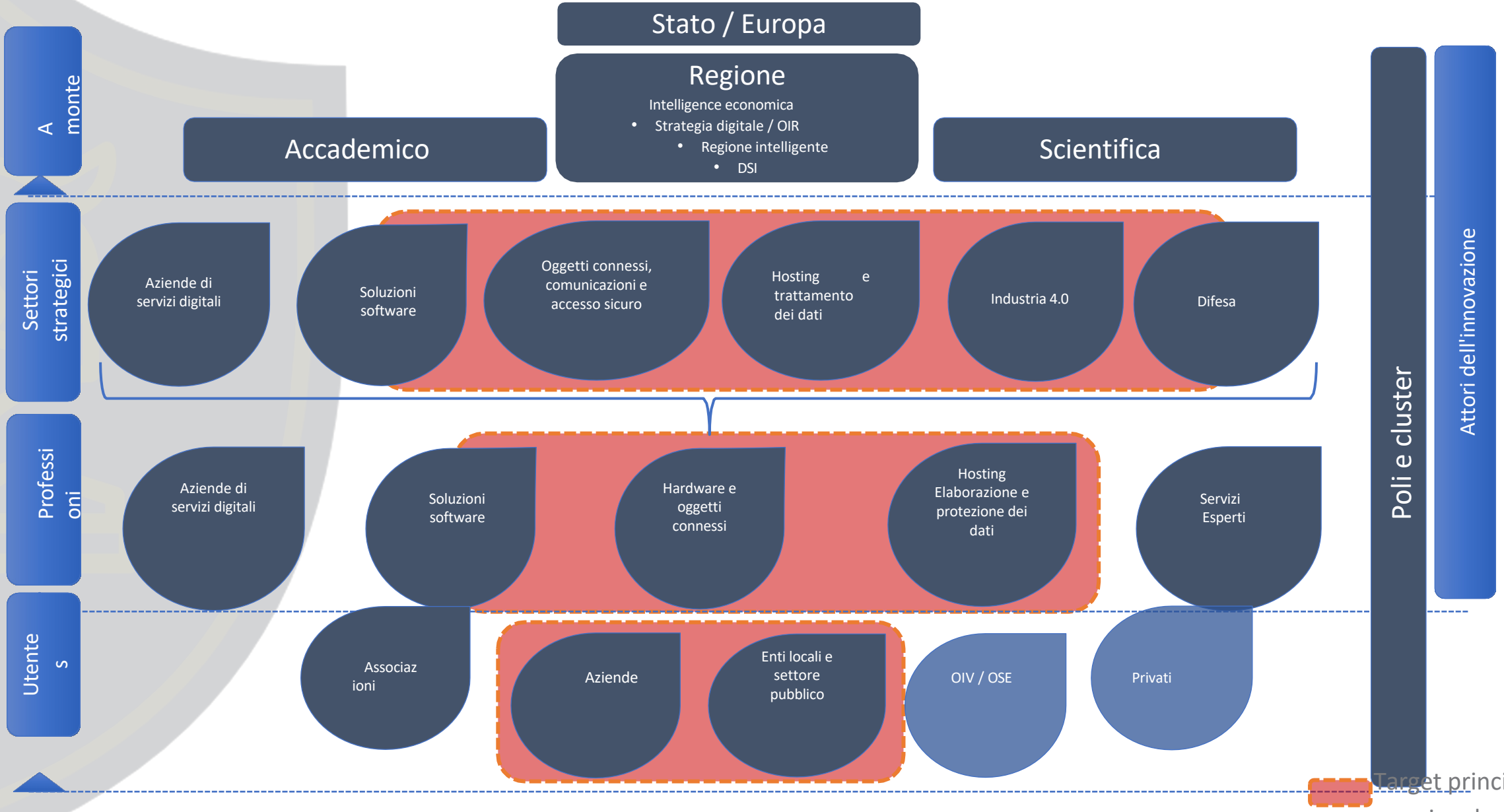


L es di agire

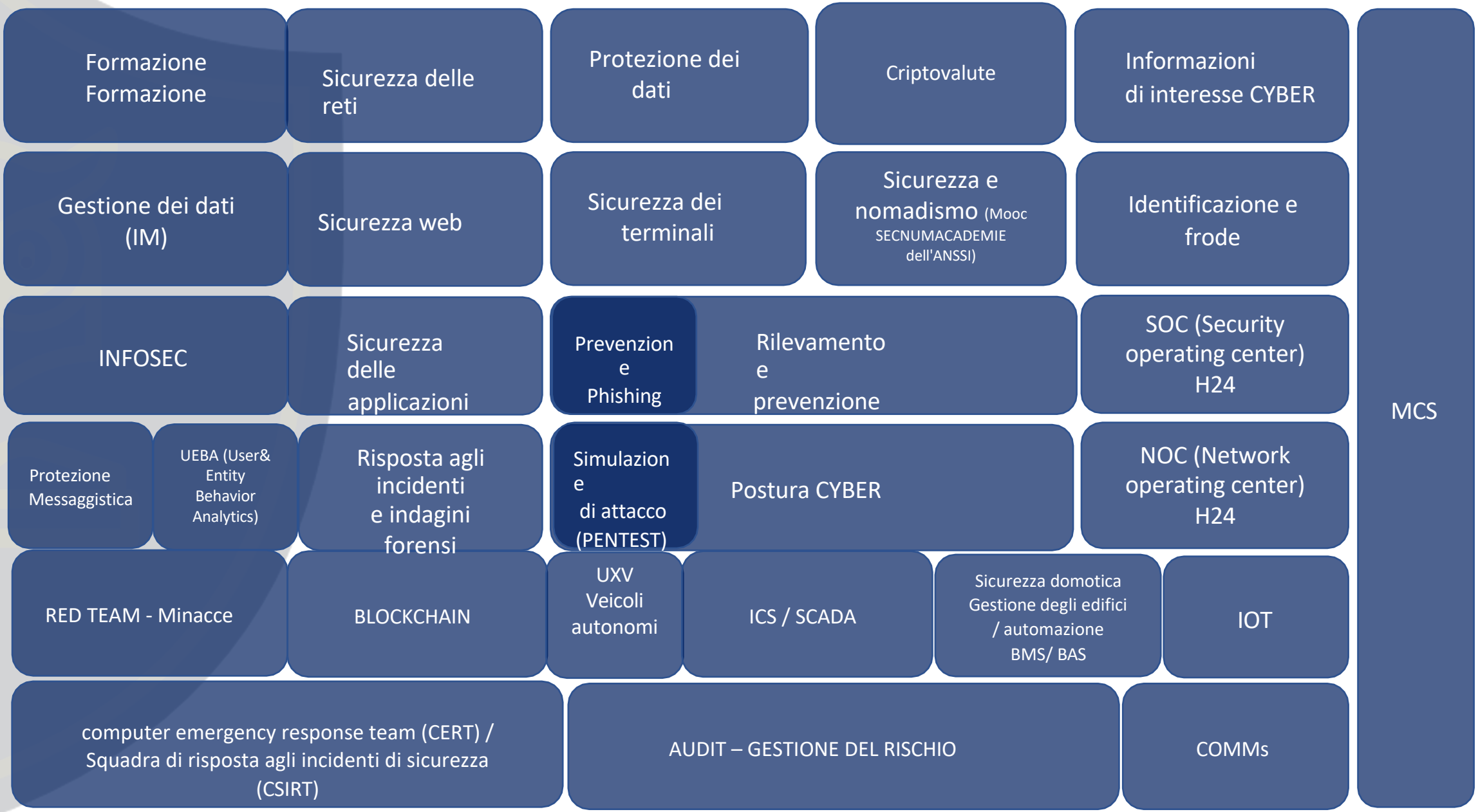
capacità

Dominio			
LEGALE	Direttiva NIS	Monitoraggio dell'applicazione nazionale della direttiva NIS da parte dei paesi membri. Specificità «Marina».	Stati membri
	Regolamentazione marittima	Studi sulle conseguenze delle normative IMO/ISPS/UE	IMO, DG MOVE, DG MARE, DG CONNECT, MS
	Leggi CYBER	Impatto delle leggi sul settore marittimo (ad esempio Cyber Act, US Cloud Act)	Commissione UE, Stati membri
SEMANTICA – STANDARD	STANDARD	Definizione e mantenimento di un "quadro semantico standardizzato" per identificare e condividere incidenti e attacchi.	ETSI, Commissione, Stati membri
	CLASSIFICAZIONE	Organizzazione degli standard di classificazione per il settore marittimo	IMO, MS
	VALUTAZIONE DEL RISCHIO	Processo standardizzato di valutazione del rischio per la comunità marittima.	IMO, ETSI, Commissione europea, MS
ORGANIZZAZIONE	CARTOGRAFIA CYBER	Implementare una cartografia delle organizzazioni marittime dell'UE per affrontare una NISD comune implementazione per il settore marittimo. La cartografia dovrebbe essere limitata	MS, Commissione
	COORDINAMENTO CYBER	Identificare una struttura di coordinamento per gestire e condividere analisi dei rischi e migliori pratiche (ad esempio mezzi di comunicazione sicuri) o l'implementazione di squadre di risposta.	Altre DG, attori dei settori economici (trasporti, logistica, lavoratori portuali, ecc.)
TECNOLOGIA	BASE TECNOLOGICA E INDUSTRIALE	Contribuire alla creazione di una base tecnologica e industriale europea per la difesa informatica.	Industria, EDA
SERVIZI	Servizi per il	Piano di servizi informatici per la sicurezza informatica di domani nella progettazione	Industria, cantieri navali, porti

Organizzazione territoriale



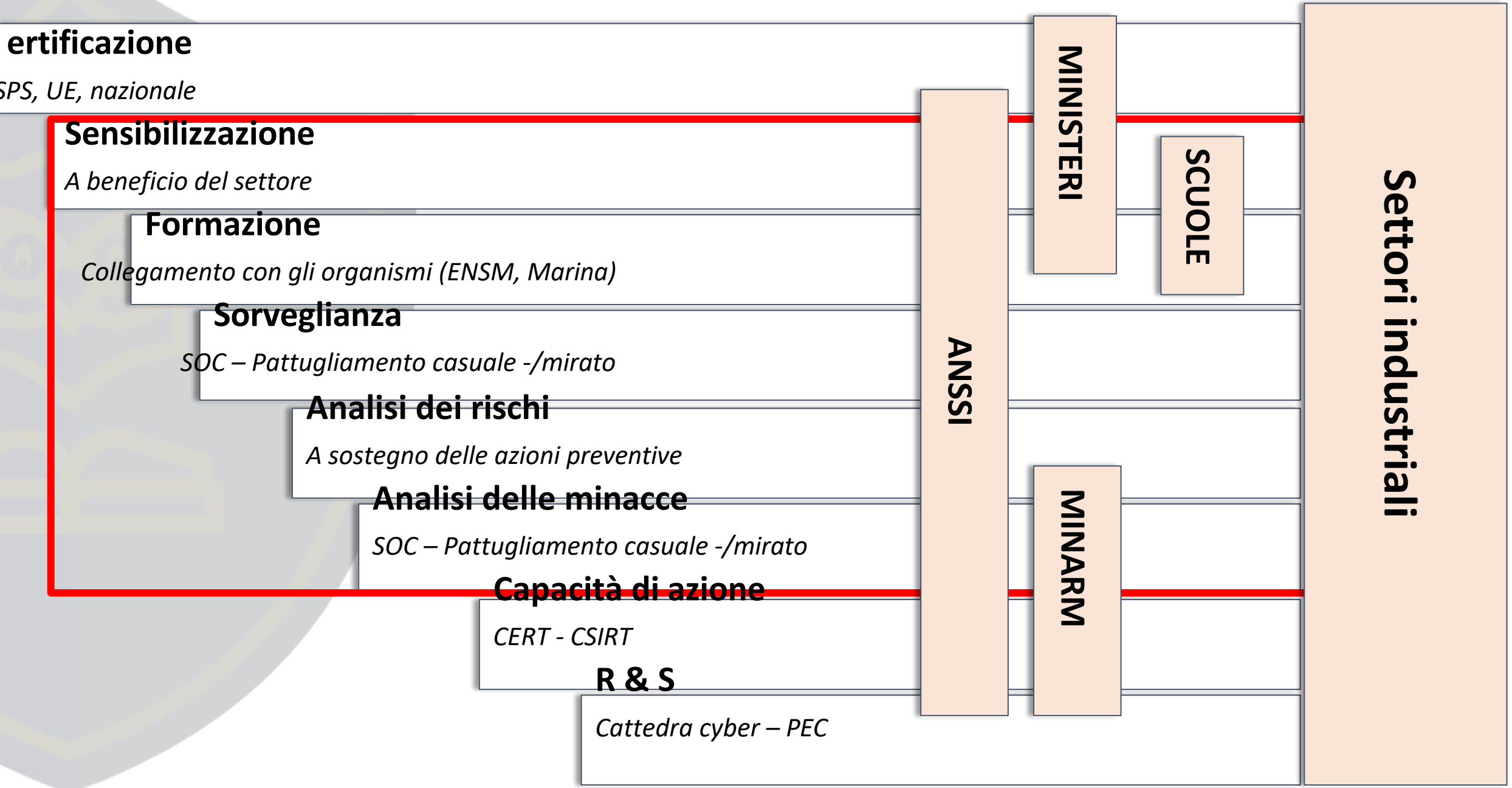
Mappatura degli operatori di sicurezza informatica



Gli attori del settore

Livello	Regolamentazione	Organismi interessati			Minacce	Osservazioni	Elementi chiave
		Porti	Navi	Attività offshore			
Organismo Importanza itale OIV) 	**ECI Direttiva (2008) LPM (2007)**	Grandi porti sicuri	Sono raramente OIV	Petrolio e gas	Attacchi informatici da parte di Stati Terrorismo Catastrofi naturali	Classificazione per settore (Energia – Trasporti) Per il settore marittimo più legato ai porti che agli operatori marittimi.	Settore sensibile. Implicazioni per la difesa Le nazioni spesso scambiano poche informazioni. I porti si sentono più OSE che OIV.
Organismo di servizi essenziali OSE) 	**NIS Direttiva (2020)**	Alcuni porti non OIV possono essere OSE	In alcuni paesi il settore marittimo comprende OSE (passeggeri)	EMR e cavi sottom arini	Terrorismo Attività criminali (comprese quelle informatiche)	All'Unione europea potrebbe essere proposta una valutazione/armonizzazione l'attuazione della direttiva NIS.	In fase di attuazione Un ostacolo all'attività economica locale non è necessariamente presa in considerazione dalla direttiva NIS
Utenti 	**RGPD (2018)**	La necessità di aumentare il PPCM della sicurezza informatica è inevitabile in un settore fortemente digitalizzato e connesso			Attività criminali Influenza	Priorità ai dati personali. Legislazione informatica poco chiara per un settore spesso trascurato e da cui proviene la minaccia	Prevenzione e formazione dei cittadini e degli organismi del settore (pesca, nautica da diporto, logistica)

Aree funzionali della sicurezza informatica



Formazione

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK: JOB PROFILES

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Legal, Policy and Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester

European Cybersecurity Skills Framework (ECSF)

Mappatura dei sistemi

gli scenari "marittimi"

Attacco generalizzato tramite compromissione di un operatore satellitare
Spionaggio

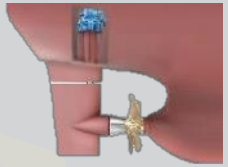
Scatenamento deliberato
di una crisi di panico
Saturazione delle reti

Modifica delle carte nautiche
(compromissione di un editore)

Modifica dei riferimenti
cartografici

Compromissione del sistema informativo
dell'armatore da una nave

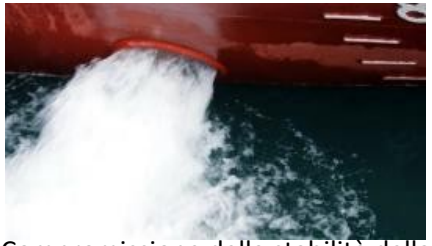
Esca GPS / Radar



Paralisi dei sistemi di
manovra

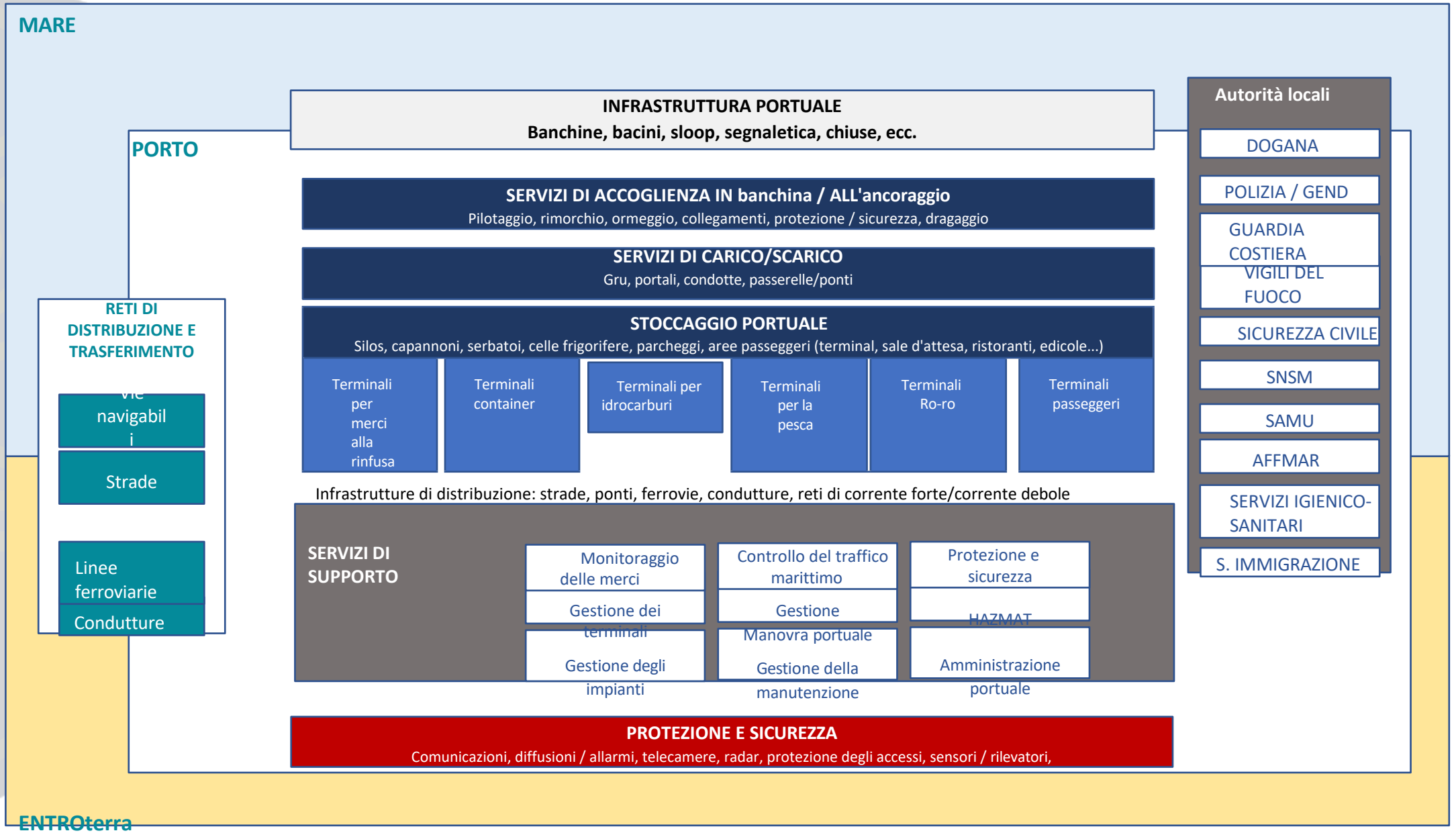
Paralisi della nave (ransomware)

Sabotaggio di una nave/flotta (attacco mirato)
Blackout energetico

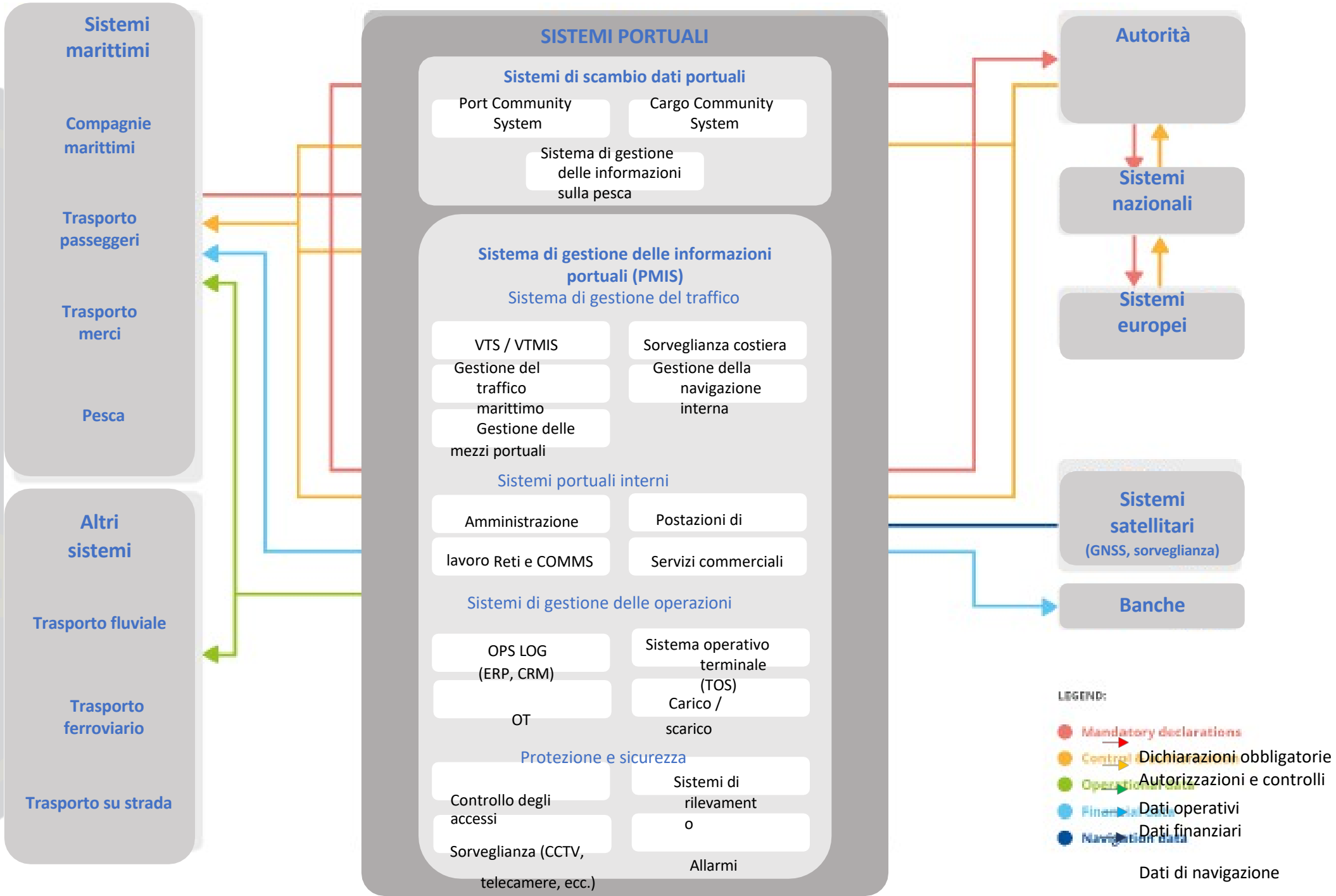


Compromissione della stabilità della nave

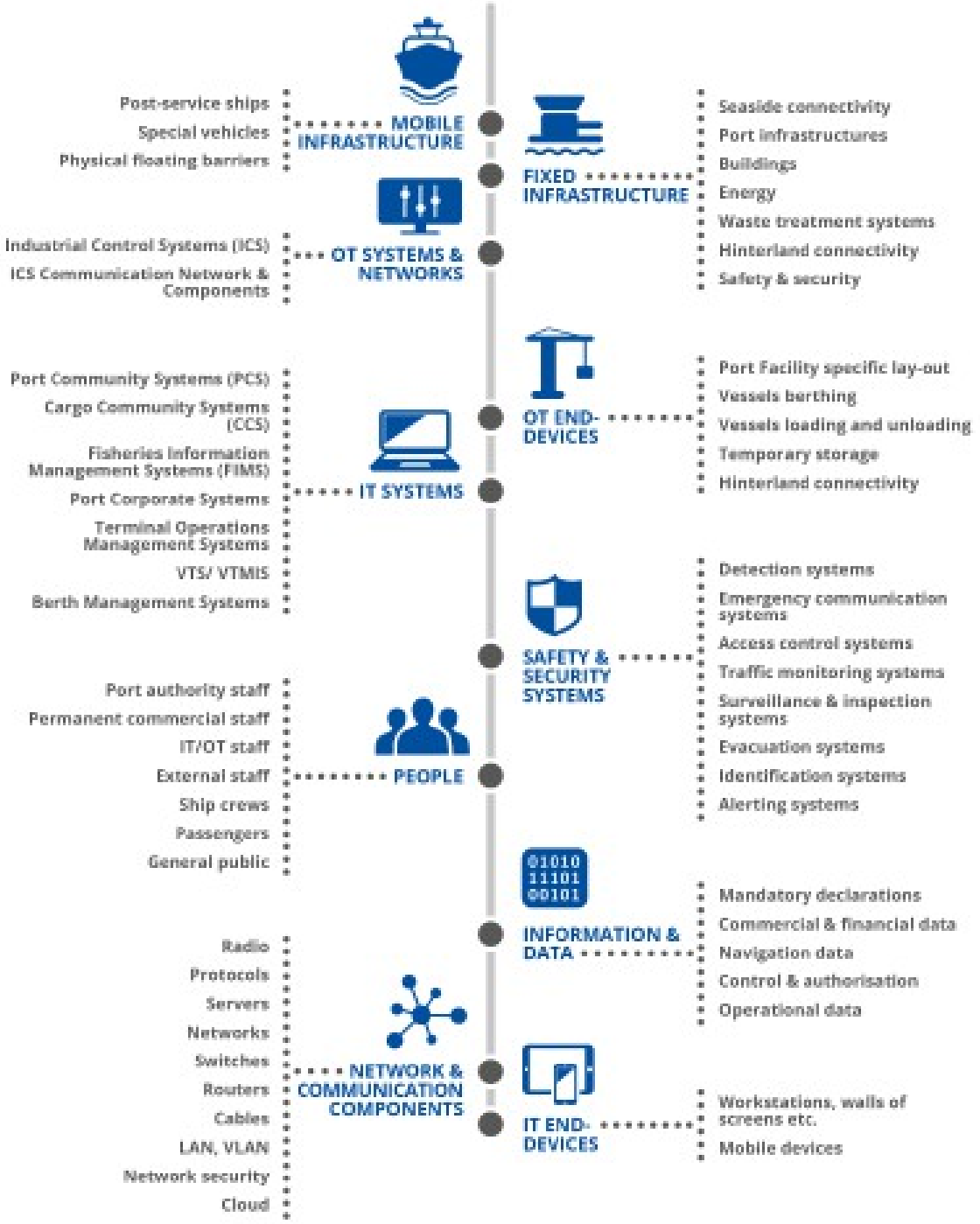
L'ecosistema portuale



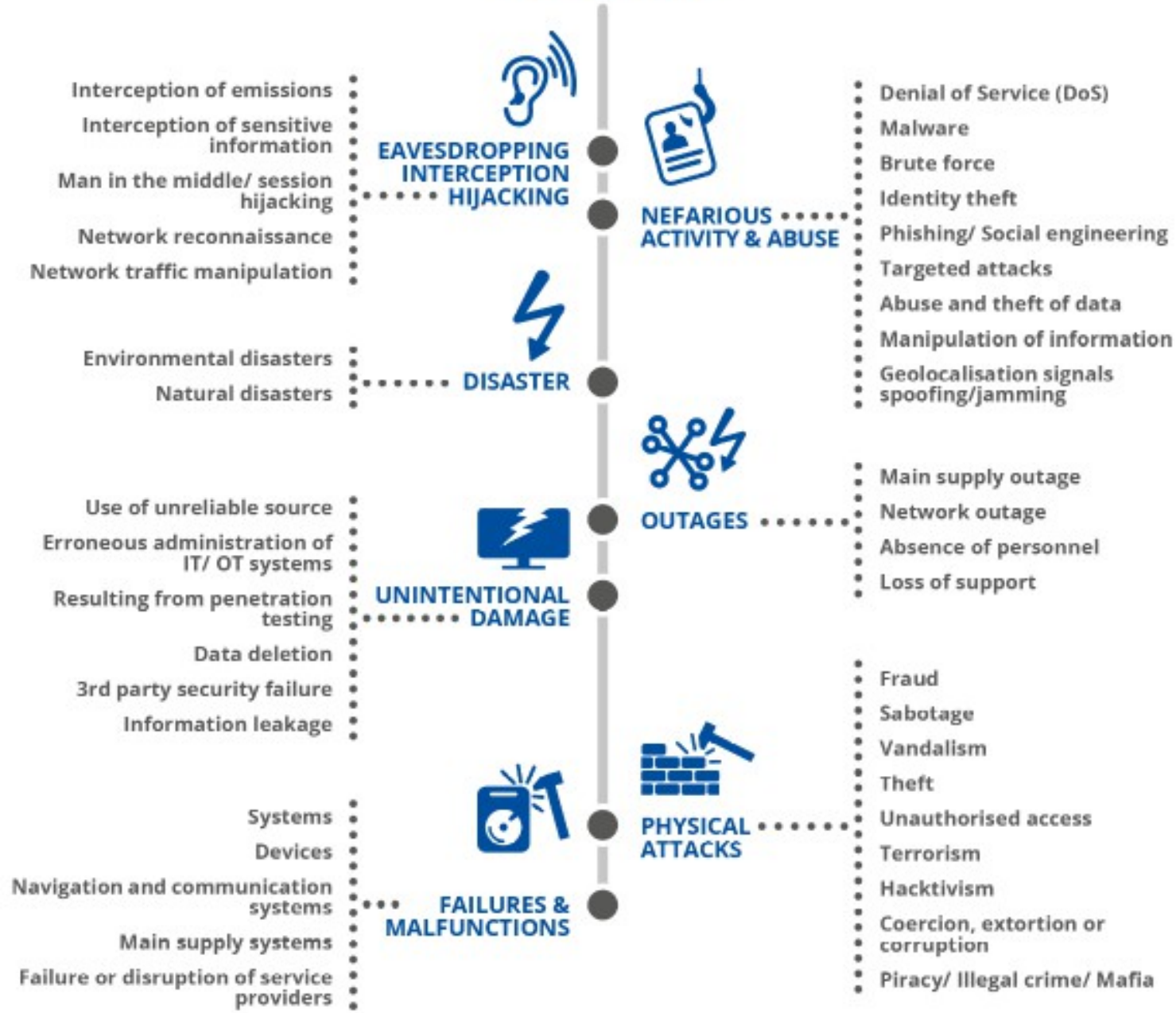
I sistemi portuali



ASSET TAXONOMY



THREAT TAXONOMY




PAUSA