WHITE PAPER - Cyber resilienza nel settore dei trasporti

Panorama degli attacchi, stato dell'arte del quadro normativo e raccomandazioni strategiche

Sommario

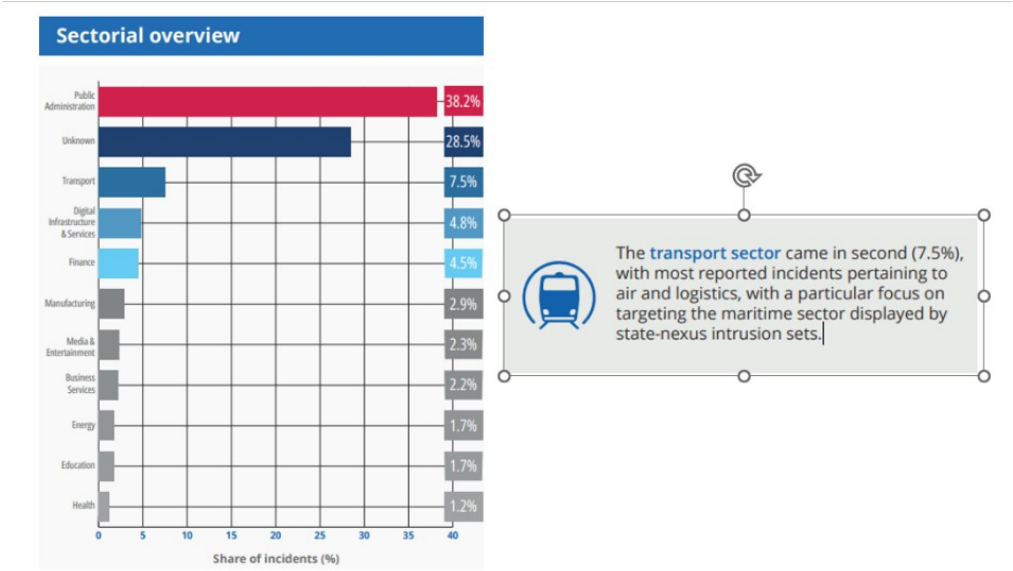
Introduzione

Il **settore dei trasporti** costituisce la **spina dorsale** dell'**economia europea e italiana**. Ferrovie, aeroporti, porti, autostrade e reti di trasporto urbano non sono soltanto infrastrutture fisiche, ma ecosistemi digitali complessi, profondamente interconnessi, che movimentano ogni giorno milioni di persone e miliardi di euro di merci. La **trasformazione digitale** accelerata in atto, con l'integrazione di **sistemi IoT, intelligenza artificiale, piattaforme cloud** e **convergenza IT/OT**, ha radicalmente **mutato** il **profilo di rischio** del settore dei trasporti, rendendolo **bersaglio privilegiato** del **crimine informatico** organizzato e degli **attori statali ostili**, considerando l'attuale contesto geopolitico. Le tensioni internazionali, il conflitto russo-ucraino e quello medio orientale tra USA-Iran-Israele e le rivalità tecnologiche tra grandi potenze hanno trasformato **le infrastrutture di trasporto** in **campo di battaglia ibrido**, dove attacchi informatici sofisticati si affiancano a tecniche di disinformazione e sabotaggio fisico.

Inoltre, le **infrastrutture critiche nei settori del trasporto** aereo, marittimo, ferroviario e stradale rientrano nel **perimetro della Direttiva NIS2**, che mira a garantire la resilienza delle infrastrutture in termini di cybersecurity, oltre che la sicurezza dei servizi e dell'intero ecosistema — produttori, fornitori, operatori — all'interno dell'Unione Europea. Senza dimenticare l'intero quadro normativo europeo in termini di sicurezza fisica e digitale a cui il settore deve conformarsi unitamente alle regolamentazioni specifiche.

Panorama degli attacchi cyber nel settore dei trasporti

Il settore dei trasporti, secondo quanto si evince dall'ultimo **Threat Landscape 2025 di ENISA**, si è classificato **secondo (7,5%).**



Fonte immagini - ENISA Threat Landscape 2025

In **Italia**, il **Rapporto CLUSIT 2026** rivela un contesto ancora più allarmante. Il **segmento trasporti e logistica** ha registrato **un aumento degli incidenti del 134,6% nel 2025** rispetto all'anno precedente, una crescita che rende la compliance alla NIS2 non più una questione di compliance formale ma una priorità strategica di sopravvivenza aziendale. Il dato italiano si inserisce in un **trend europeo preoccupante**: gli **attacchi ransomware** sono **aumentati del 92% in Europa** nell'ultimo trimestre del **2025**, con il settore logistico-trasportistico che rappresenta uno dei segmenti più vulnerabili.

Il **Global Risk Management Survey 2025 di Aon**, che ha coinvolto quasi 3.000 rispondenti in 63 Paesi, ha identificato i **cyberattacchi e le violazioni dei dati** come il **rischio più grave** per il **settore trasporti e logistica**. Il **17,7% delle aziende di trasporto** ha subito **perdite** legate a cyberattacchi negli ultimi 12 mesi — una percentuale superiore persino ai rischi macroeconomici o alle interruzioni operative. L'**85,3% delle organizzazioni** ha implementato **procedure formali** per la gestione del **rischio informatico**, il valore più alto tra tutte le categorie di rischio monitorate.

Indicatore	Dato
Quota incidenti cyber UE (trasporti)	11,19% — Secondo settore più colpito (ENISA 2024)
Incidenti con origine dolosa (CIRAS 2023)	60% del totale settore trasporti
Crescita incidenti IT/logistica in Italia (2025)	+134,6% rispetto all'anno precedente (Rapporto Clusit 2026)
Crescita ransomware in Europa (Q4 2025)	+92% su base annua
Aziende trasporti con perdite cyber (12 mesi)	17,7% (Aon Global Risk Survey 2025)
Attacchi ransomware in Polonia Q1 2025	+126% su base annua (Check Point Research)
Incidenti con origine da fornitori esterni	30% del totale (dato crescente)

Tipologie di attacco prevalenti nel settore trasporti

Di seguito le più comuni tipologie di attacco ai danni del settore dei trasporti.

Ransomware

Il ransomware rappresenta la **minaccia principale** per il settore. Il meccanismo tipico prevede l'**infiltrazione** nella rete aziendale — spesso attraverso credenziali rubate o vulnerabilità nei sistemi di fornitori terzi — la **cifratura dei dati operativi critici** e la richiesta di un **riscatto**. La variante della **"doppia estorsione"** aggiunge alla cifratura la minaccia di **pubblicazione dei dati sensibili** sottratti, moltiplicando la pressione sulle organizzazioni.

Di fatto, esiste nel mercato una **regola non scritta delle 48 ore**: due giorni senza accesso ai sistemi significano un **completo blocco operativo**, con l'accumulo di pesanti **penali contrattuali**. I cybercriminali conoscono perfettamente questo meccanismo e lo sfruttano per **massimizzare la pressione sul management**, spingendo verso il **pagamento del riscatto** anche in assenza di garanzie sul ripristino dei dati.

DDoS e hacktivismo

Gli attacchi **Distributed Denial of Service (DDoS)** rappresentano la **tipologia più comune** nel settore dei trasporti, spesso orchestrati da **gruppi hacktivisti** con motivazioni politiche o ideologiche. Le **reti di trasporto pubblico** locale sono diventate **bersagli prioritari** per chi cerca visibilità, colpendo sistemi di biglietteria e app informative per causare disagi visibili ai cittadini. Esempi recenti includono attacchi ad ATAC Roma e Czech Railways. Senza dimenticare il cyberattacco di fine 2025 che aveva preso di mira Collins Aerospace (fornitore di servizi per i sistemi di check-in e imbarco), aveva comportato le operazioni automatizzate in diversi importanti scali europei, tra cui Bruxelles, Berlino e Heathrow a Londra. Oppure l'attacco informatico a dicembre 2025 contro l'Autorità di sistema portuale del mare Adriatico centrale, con parziale sottrazione di dati.

Supply chain attacks e minacce n-th party

Gli **attacchi alla supply chain** rappresentano una delle **minacce in più rapida crescita**. Anziché colpire direttamente il grande operatore di trasporto — solitamente ben protetto — i criminali prendono di mira i suoi fornitori di secondo e terzo livello, spesso con posture di sicurezza molto più deboli. Il report **2025 Supply Chain Cybersecurity Trends** indica che l'88% dei responsabili della sicurezza teme un attacco attraverso la catena di fornitura e oltre il **70% delle organizzazioni** ha vissuto almeno **un incidente importante nell'ultimo anno** che ha coinvolto i propri **fornitori**.

Il problema delle cosiddette **minacce da "n-th party"** — partner di secondo e terzo livello su cui non esiste un reale controllo — è **strutturale**: il **79% delle aziende monitora per la cybersicurezza meno della metà della propria supply chain**, operando nell'illusione del controllo.

Phishing, Spoofing e Infostealer

Le **tecniche di phishing e spoofing** — l'impersonificazione di soggetti legittimi per rubare dati o prendere il controllo dei carichi — rimangono il **vettore di ingresso più comune**. Secondo le analisi di settore, oltre il **90% delle violazioni di dati** inizia con l'uso di **malware "infostealer"** che rubano le **credenziali dei dipendenti**, spesso dai loro PC domestici mentre lavorano da remoto. Queste credenziali vengono poi vendute nei mercati del Dark Web ai gruppi ransomware, che le utilizzano per accedere ai sistemi aziendali.

Inoltre, i modelli linguistici di grandi dimensioni vengono impiegati per creare **campagne di spearphishing personalizzate**, con email indistinguibili da comunicazioni legittime, in grado di ingannare anche dipendenti formati alla sicurezza informatica. Sia **Europol** sia **ENISA** avvertono di una progressiva **professionalizzazione del mercato della criminalità**, con **servizi di hacker-for-hire**, **malware-as-a-service** e **DDoS-as-a-service** disponibili a prezzi accessibili.

Impatti secondari ed effetti a cascata derivanti da attacchi cyber

È fondamentale, quando si sviluppa un **piano di continuità aziendale** o di **disaster recovery tenere conto** non soltanto dell'**impatto diretto dell'attacco**, ma anche degli **effetti secondari** e delle **interdipendenze interne**. I cyberattacchi causano frequentemente **danni collaterali** che vanno ben oltre il sistema inizialmente colpito, innescando **reazioni a catena** che si verificano all'interno delle reti interne.

Ad esempio, una violazione di sistemi IT aziendali — email, sistemi di gestione dell'identità, infrastrutture di rete — può interrompere i sistemi OT anche se questi rimangono tecnicamente non compromessi, semplicemente perché i due mondi condividono infrastrutture di autenticazione o comunicazione. Queste **interdipendenze interne**, se trascurate nella fase di pianificazione, possono **compromettere** gli sforzi di **continuità operativa** e **ritardare** significativamente il **recupero.**

Gli impatti secondari più rilevanti per il settore dei trasporti includono:

- La **corruzione o perdita di dati operativi critici** (manifesti di carico, piani di volo, orari ferroviari).
- Le **interruzioni di servizi digitali per i passeggeri** (app, biglietterie, sistemi di informazione).
- I **danni economici** da fermo operativo, penali contrattuali e perdita di fiducia dei clienti.
- Le **violazioni della privacy** nei programmi di fidelizzazione
- I **danni fisici** in scenari estremi, quando gli attacchi raggiungono i sistemi OT di controllo (segnalamento ferroviario, sistemi di gestione del traffico aereo.
- L'**erosione della fiducia dei passeggeri**, un asset reputazionale fondamentale in un settore ad alta concorrenza.

Analisi dei vari settori dell'ecosistema trasporti: maturità, criticità e vulnerabilità

Il settore dei trasporti dell'UE è suddiviso in **quattro sottosettori chiave** secondo la Direttiva **NIS2**: **aviazione, ferroviario, marittimo e stradale**.

Inoltre, ogni sottosettore presenta un profilo di **rischio**, un livello di **maturità cyber** e una struttura di **governance molto differenti**. Tale eterogeneità è uno dei fattori che rendono complessa l'applicazione uniforme dei requisiti normativi europei.

Vediamo di seguito lo **stato dell'arte** secondo quanto scaturisce dal **Rapporto ENISA NIS 360** pubblicato lo scorso maggio 2025 sullo stato di recepimento della NIS1.

SETTORE AEREO: maturità elevata, ma ecosistemi complessi

Il sottosettore dell'aviazione è leader nella cybersicurezza tra i trasporti, grazie a un ecosistema normativo strutturato.
La **Direttiva NIS2** si affianca a **regolamenti specifici** che offrono un quadro dettagliato per la gestione dei rischi di sicurezza delle informazioni, supportato dall'**EASA**.

Nonostante la maturità superiore, il **settore aereo** è quello che detiene la **quota maggiore di incidenti** osservati in termini assoluti. La ragione è strutturale: un aeroporto non è una singola entità ma un insieme di vettori, operatori di terra, controllo del traffico aereo e servizi cargo. Una vulnerabilità in un solo fornitore della catena può paralizzare l'intero scalo.
Inoltre, l'uso pervasivo di IoT per il monitoraggio dei bagagli, passaporti elettronici e sistemi di gestione degli edifici (*BMS – Building Management System*) offre molteplici punti di ingresso. **Darktrace** ha documentato **attacchi avanzati** in cui i criminali hanno utilizzato tecniche di **ARP (Address Resolution Protocol) spoofing** per dirottare sistemi di gestione aeroportuale e reti di riconsegna bagagli.

Le **motivazioni geopolitiche** rappresentano un **fattore aggiuntivo**: attori statali, come gruppi legati all'Iran documentati da ENISA, prendono di mira il settore aerospaziale per spionaggio e interruzioni operative, utilizzando **campagne di spearphishing** mirate contro personale tecnico e operativo. L'iniziativa **ECCSA (European Center for Cybersecurity in Aviation)** e il network **NoCA (Network of Cybersecurity Analysts)**, promossi dall'**EASA (European Union Aviation Safety Agency**), rappresentano le principali strutture di **condivisione delle informazioni e risposta coordinata** del settore

Parola all'esperto del settore - Alberto Caruso de Carolis – Membro del Consiglio Direttivo di AIIC (Associazione Italiana per le Infrastrutture Critiche)

Secondo quanto afferma **Alberto Caruso de Carolis,** "il settore aeroportuale italiano presenta una maturità cyber avanzata, avendo adottato standard come la ISO 27001 ben prima degli obblighi della Direttiva NIS. L'approccio strategico fin dall'inizio adottato dagli operatori nazionali, non considera la cybersecurity come una disciplina isolata, ma come una declinazione strutturale di pilastri già consolidati: *Aviation Safety* (sicurezza del volo) e *Aviation Security* (protezione da atti illeciti), per la natura stessa del settore all'attenzione per l'innovazione tecnologica e per la naturale sensibilità al "risk management".

"Questa integrazione - come sottolinea De Carolis - permette di considerare la gestione del rischio informatico all'interno di modelli organizzativi di settore esistenti, con una *accountability* ben precisa e di cui verosimilmente la Direttiva NIS2 ne ha tratto ispirazione. Infine, la resilienza del comparto è sostenuta da rigorosi programmi di formazione previsti dal Programma Nazionale di Formazione e Certificazione per la Sicurezza dell'Aviazione Civile, adottato dall'Ente Nazionale per l'Aviazione Civile (ENAC), a seguito di apposita modifica del Regolamento di esecuzione (UE) n. 2015/1998".

I corsi, differenziati per categorie di personale, spaziano dalla *risk awareness* di base alla gestione specialistica degli eventi cyber. Tale visione trasversale, profondamente assimilata dal settore, è ritenuta essenziale per contrastare le minacce alla continuità di un'infrastruttura vitale per il Paese quale quella del settore Aviation.

De Carolis evidenzia come, a suo avviso, "la tradizionalmente elevata attenzione agli standard di sicurezza nel settore del trasporto aereo – nelle sue diverse declinazioni di safety, security e cybersecurity – ha trovato una risposta organica non solo nella Direttiva 2555 (NIS2), ma soprattutto nell'adozione della Direttiva 2557 (CER) sulla resilienza dei soggetti critici. Quest'ultima recepisce, in larga misura, i principi multisettoriali propri dell'Aviation, estendendoli, in un'ottica olistica, a tutte le filiere delle infrastrutture critiche e alle loro interdipendenze, contribuendo così a superare le criticità che non risultano governabili all'interno dei soli perimetri aeroportuali".

SETTORE FERROVIARIO: convergenza IT/OT e sistemi legacy

Il settore ferroviario si posiziona al **secondo posto per maturità cyber**, guidato dalla **Direttiva NIS2** e dal **Cyber Resilience Act**. L'armonizzazione tra Stati membri è essenziale per evitare il sovraccarico dei requisiti di compliance. Supportato dall'**European Union Agency for Railways (ERA)**, il settore sta mappando i requisiti normativi con gli standard internazionali, in particolare il **CENELEC CLC/TS 50701:2023**, che rappresenta il **framework** fondamentale per la **gestione della cybersicurezza ferroviaria**, coprendo sia il materiale rotabile che le installazioni fisse.

La **sfida principale** del settore ferroviario è la **convergenza IT/OT**: la fusione tra le reti informatiche aziendali e le tecnologie operative che controllano il movimento dei treni e il segnalamento crea punti critici di vulnerabilità. Molti sistemi OT sono stati progettati decenni fa **senza criteri di sicurezza nativa** e hanno **cicli di vita lunghissimi**, rendendo difficile l'applicazione di patch senza interrompere il servizio.

È importante evidenziare che l'implementazione dell'**ERTMS (European Rail Traffic Management System)** nei principali corridoi europei porta **benefici di efficienza ma introduce nuove superfici di attacco** che devono essere gestite con attenzione.

Un aspetto critico emerso dal documento di analisi di ENISA è che il settore ferroviario **effettua raramente valutazioni della sicurezza informatica, piani di risposta agli incidenti e test di ripristino**, oppure lo fa in modo discontinuo. Inoltre, molti operatori impiegano oltre tre mesi per correggere le vulnerabilità note, mentre gli aggressori le sfruttano in pochi giorni — una finestra di esposizione inaccettabile per infrastrutture critiche.

Il tema **safety vs. security** assume nel ferroviario una **dimensione particolarmente critica**: a differenza dei guasti meccanici prevedibili e gestibili attraverso procedure consolidate, le **minacce cyber** sono **dinamiche e intenzionali**. Un attacco ai sistemi di segnalamento o controllo non mette a rischio solo i dati, ma la vita stessa dei passeggeri. Per il **2026** è prevista l'introduzione dello **standard IEC 63452**, che rafforzerà ulteriormente il legame tra sicurezza fisica e informatica nel settore ferroviario.

Parola all'esperto del settore – Christian Lusi – Dirigente in ANSFISA (Agenzia Nazionale per la Sicurezza delle Ferrovie e delle Infrastrutture Stradali e Autostradali)

"È indubbio - come sottolinea **Christian Lusi** - che, in ambito ferroviario, la superficie esposta ad attacchi cyber aumenterà esponenzialmente nei prossimi anni.
Ciò è dovuto, da un lato, al sempre maggiore utilizzo di sensoristica IoT installata sull'infrastruttura e sui veicoli per rilevare l'insorgere di anormalità (i.e. accelerometri per rilevare vibrazioni anomale delle rotaie, captatori di emissione acustiche per rilevare la formazione di cricche nel metallo, sensori di livello per monitorare la geometria del binario, sonde a riflettometria nel dominio del tempo per rilevare fenomeni di ammaloramento della massicciata, fibre ottiche rese solidali alla rotaia per monitorarne la termica, ecc.) e, dall'altro lato, alla realizzazione di un sistema di telecomunicazioni che renderà possibile il trasporto, verso i centri di elaborazione, dell'enorme mole di dati prodotti da tali sensori, costituito da una rete radiomobile 5G

a copertura dell'intera rete ferroviaria, basata sul sistema europeo *FRMCS (Future Railway Mobile Communication System*). Un sistema attualmente in corso di specificazione e da installare prevedibilmente entro il 2035, anno in cui i fornitori dell'attuale sistema GSM-R smetteranno di produrre tale tecnologia (che ricordiamo essere ancora di tipo 2G)".

Inoltre, Lusi aggiunge: "Le ben note vulnerabilità dei suddetti sistemi IoT (celebre al riguardo la ricerca di Kaspersky Lab del 2017) e 5G (si rammenti il rapporto del 2019 con cui il COPASIR richiamava l'attenzione sulle backdoor introdotte dai vendor asiatici) richiederà uno sforzo enorme a tutti i soggetti coinvolti (la cui molteplicità rappresenta un ulteriore elemento di criticità) – a mio parere – che dovrà procedere secondo le seguenti linee strategiche:

- attribuire, ai soggetti coinvolti, le risorse umane e strumentali e le competenze tecniche necessarie;
- chiarire nel dettaglio compiti, responsabilità e "procedure di interfaccia" tra tutti gli attori, inclusi quelli istituzionali sia a livello nazionale sia a livello europeo;
- incentivare, nella definizione di strategie e di linee d'azione, il coinvolgimento, da parte degli organi istituzionalmente competenti, di altri soggetti con competenze non dirette in materia di cybersecurity - ma comunque detentori di *know-how* specialistico riguardo ai settori e ai sistemi oggetto di possibili attacchi".

SETTORE MARITTIMO: zona di rischio e dipendenze geopolitiche

Il sottosettore marittimo soffre di **carenze** significative in materia di **governance, competenze informatiche** e **gestione delle vulnerabilità**. L'**European Maritime Safety Agency (EMSA**), che nel 2024 ha pubblicato linee guida per l'armonizzazione della sicurezza marittima, e lo **STAKEHOLDER Advisory Group on Maritime Security (SAGMAS)** rappresentano i principali strumenti di supporto.

Il **settore marittimo** è entrato in quella che gli analisti definiscono una **"zona di rischio"**, dove il livello di importanza strategica supera nettamente l'attuale maturità dei sistemi di difesa cyber.
I **porti europei** affrontano **sfide** legate alla **dipendenza tecnologica** da **fornitori extra-UE**, in particolare dalla **Cina**, che funge simultaneamente da proprietario di infrastrutture portuali, investitore e fornitore di attrezzature tecnologiche. Esiste il timore fondato che **tale dipendenza** possa essere sfruttata per **attività di spionaggio industriale** o per **interruzioni deliberate** attraverso la coercizione economica in scenari di tensione geopolitica.

Inoltre, l'introduzione di **navi autonome (Maritime Autonomous Surface Ships — MASS)** introduce **nuovi profili di rischio** legati ai centri di controllo remoto e ai sistemi di navigazione basati su sensori.

Ancora, la **criticità temporale** del settore marittimo è **la più alta** tra tutti i sottosettori: gli **incidenti informatici** che colpiscono le operazioni portuali possono avere **ripercussioni immediate e diffuse sulle catene di approvvigionamento**, con effetti a cascata su merci deperibili, materie prime energetiche e produzione just-in-time. Il **rischio di spoofing** del **sistema AIS (Automatic Identification System)** è oggetto di specifici gruppi di lavoro EMSA e rappresenta una **minaccia concreta** per la sicurezza della navigazione.

Parola all'esperto del settore - Federica Montaresi - Segretario Generale AdSP Mar Ligure Orientale

"I porti oggi – come evidenzia **Federica Montaresi** - si trovano ad affrontare una duplice sfida: da un lato la necessità di accelerare la digitalizzazione e l'automazione dei processi per essere efficienti e poter rispondere ai cambiamenti di scenario che impattano sulle supply chain, dall'altro l'esigenza strategica di proteggere reti e sistemi da possibili attacchi cyber che diventano sempre più frequenti anche in relazione al contesto geopolitico attuale.

La sicurezza della supply chain tecnologica diventa, quindi, un elemento di sovranità nazionale ed europea, evidenziando la necessità di rafforzare standard comuni, progetti di cooperazione e soluzioni tecnologiche affidabili e interoperabili".

Montaresi aggiunge: "Il settore marittimo mostra ancora significative carenze sul piano della governance della sicurezza informatica e delle competenze digitali, soprattutto nei contesti portuali e logistici.
La crescente integrazione tra sistemi IT e OT, spesso non accompagnata da adeguate strategie di gestione delle vulnerabilità, espone infrastrutture critiche a rischi sistemici. In molti casi la cybersecurity è trattata come un adempimento tecnico e non come una componente strutturale e di governance strategica della sicurezza marittima, con insufficiente coinvolgimento dei vertici decisionali e una limitata cultura del rischio cyber tra operatori e personale.
Per questo è sempre più necessario diffondere nelle proprie aziende e negli Enti come le Autorità di Sistema Portuale una vera e propria cultura della cybersicurezza sensibilizzando in modo trasversale tutti gli uffici della struttura organizzativa".

Inoltre, Montaresi evidenzia: "Gli impatti di un incidente informatico che colpisce un porto possono essere diversi e gravosi con ripercussioni immediate e rilevanti sulla movimentazione delle merci e sull'approvvigionamento di materie prime energetiche. I porti, in qualità di infrastrutture strategiche nazionali, sono i nodi della catena logistica dove transita una mole di dati da quelli energetici a quelli ambientali, a quelli commerciali, doganali e logistici.
Il blocco dei sistemi di gestione portuale o dei terminal può interrompere catene logistiche complesse, generando ritardi, congestioni e aumenti dei costi, con effetti a cascata sull'economia reale.
In un contesto in cui una quota rilevante del commercio e dell'energia transita via mare, la resilienza cyber dei porti non è solo una questione tecnica, ma un fattore chiave di stabilità economica e sicurezza nazionale".

SETTORE STRADALE: il sottosettore più vulnerabile

Il sottosettore stradale si colloca **all'ultimo posto per maturità cyber** tra i quattro comparti. Manca di un supporto normativo mirato, di iniziative di condivisione delle informazioni strutturate e di piani documentati e testati di risposta agli incidenti.
Paradossalmente, il sottosettore stradale è il **meno avanzato digitalmente** ma è quello con la **traiettoria di crescita del rischio più ripida**: con l'adozione graduale degli **ITS (Intelligent Transport Systems), per la gestione del traffico** e i **servizi di informazione in tempo reale**, la **superficie di attacco si espande rapidamente**, senza che vi sia una corrispondente crescita della postura di sicurezza.

Gli standard come **ISO 21434** interamente dedicato alla **cyber security dei veicoli** e i **regolamenti UNECE R155-156** si applicano ai **veicoli connessi** sul versante automotive, ma non coprono adeguatamente le infrastrutture stradali fisse e i sistemi di controllo del traffico.

Parola all'esperto del settore - Giuseppe Orsini- Funzionario in ANSFISA (Agenzia Nazionale per la Sicurezza delle Ferrovie e delle Infrastrutture Stradali e Autostradali)

Come afferma **Giuseppe Orsini**: "Il settore stradale si trova oggi in una fase di profonda trasformazione tecnologica che, proprio perché ancora in larga parte in evoluzione, rappresenta un'opportunità strategica per costruire fin dall'origine un robusto modello europeo condiviso di governance della sicurezza digitale della mobilità e delle infrastrutture connesse.
La diffusione delle Smart Road, dei sistemi ITS (*Intelligent Transport Systems*), di innovative piattaforme digitali di gestione del traffico e dei sistemi V2X (*Vehicle-to-Everything*) sta trasformando la rete stradale in un ecosistema cyber-fisico integrato, nel quale cybersecurity e safety risultano sempre più interdipendenti".

Inoltre, Orsini aggiunge: "Un altro importante settore è monitoraggio infrastrutturale — strutturale, sismico, idraulico e geotecnico — la protezione dei dati provenienti dai sistemi che concorrono alla valutazione dello stato di salute delle opere e alla gestione della sicurezza delle reti stradali. La compromissione o alterazione

di tali dati potrebbe infatti incidere direttamente sulla capacità decisionale degli enti gestori e sulla continuità operativa delle infrastrutture.
In tale contesto risulta essenziale sviluppare una politica comune europea capace di coordinare ricerca, sviluppo, gestione operativa e standardizzazione attraverso la collaborazione tra gli Stati membri, così da garantire interoperabilità, continuità territoriale ed efficienza operativa lungo la rete europea dei trasporti, riducendo al contempo la dipendenza da tecnologie e fornitori extra-UE.

Un esempio concreto di integrazione europea è rappresentato dalla piattaforma *C-Roads*, iniziativa congiunta della Commissione Europea, degli Stati membri e dei principali gestori infrastrutturali per lo sviluppo armonizzato dei sistemi C-ITS (*Cooperative Intelligent Transport Systems*) lungo la rete TEN-T".

Orsini altresì evidenzia: "Attraverso standard tecnici comuni, sperimentazioni operative e servizi interoperabili di comunicazione tra veicoli, infrastrutture e centrali di controllo, il programma ha già consentito l'implementazione di sistemi di allerta, gestione dinamica del traffico e cooperazione V2X su scala transfrontaliera. Tale modello di governance tecnica e operativa potrebbe costituire un riferimento anche per i futuri sistemi digitali di monitoraggio e gestione delle infrastrutture stradali. Integrandosi progressivamente con il quadro normativo europeo in materia di cybersecurity e resilienza definito dalla Direttiva NIS2, dal Cyber Resilience Act (CRA), dall'AI Act e dalla Direttiva CER (Critical Entities Resilience).

La sfida della cybersecurity nel settore stradale non riguarda quindi soltanto la protezione delle infrastrutture digitali, ma la capacità dell'Europa di accompagnare in modo sicuro l'integrazione sempre più stretta tra mobilità, veicoli connessi e infrastrutture stradali, garantendo continuità operativa, interoperabilità e sicurezza dell'intero ecosistema dei trasporti".

Sottosettore	Maturità Cyber	Principale Vulnerabilità
Aviazione	Alta (leader di settore)	Complessità ecosistema, motivazioni geopolitiche
Ferroviario	Media-Alta	Sistemi legacy OT, frequenza test inadeguata
Marittimo	Media (zona di rischio)	Dipendenze extra-UE, gap governance
Stradale	Bassa	Assenza supporto normativo mirato, ITS non protetti

Il quadro normativo europeo: la NIS2 e oltre

Di seguito una panoramica del quadro normativo che impatta sul settore dei trasporti andando oltre la NIS2.

NIS 2 – Il pilastro della cyber resilienza

La Direttiva NIS2 rappresenta la risposta legislativa più ampia e strutturata dell'Unione Europea all'aumento della minaccia cyber alle infrastrutture critiche. Adottata nel novembre 2022 in sostituzione della precedente Direttiva NIS del 2016, essa estende significativamente il perimetro di applicazione, innalza i requisiti minimi di sicurezza e introduce meccanismi di enforcement molto più stringenti.

Per il settore dei trasporti, la NIS2 rappresenta una svolta paradigmatica. Il **settore** è classificato come **"settore ad alta criticità" nell'Allegato I,** il che significa che le organizzazioni che vi appartengono sono soggette al **regime più rigoroso di obblighi e controlli**. Il perimetro di applicazione comprende: nel trasporto aereo, vettori aerei commerciali, enti di gestione aeroportuale e operatori del controllo del traffico aereo; nel ferroviario, gestori dell'infrastruttura e imprese ferroviarie; nel marittimo, società di navigazione, autorità portuali e servizi di gestione del traffico marittimo; nel stradale, autorità di gestione stradale e operatori di sistemi di trasporto intelligenti.

Recentemente, il **Ministero delle Infrastrutture e dei Trasporti (MIT)** ha aggiornato le **misure di sicurezza per i porti e le navi nazionali** con la Circolare 177/2025, integrando la cybersicurezza nei codici internazionali **ISM (International Safety Management)** e **ISPS (International Ship and Port Facility Security)** — un esempio di come la normativa settoriale specifica si coordini con il quadro NIS2.

Cyber Resilience Act (CRA)

Il regolamento CRA, adottato nell'ottobre 2024 e applicabile progressivamente fino al 2027, rappresenta una rivoluzione nella **regolamentazione della sicurezza dei prodotti digitali.** Per la prima volta nell'ordinamento europeo, viene introdotto un obbligo di **sicurezza by design per tutti i prodotti con elementi digitali** (hardware e software) immessi sul mercato UE.

L'impatto del CRA sul settore dei trasporti è molto rilevante. I **produttori** di sistemi avionici, di apparati di segnalamento ferroviario, di software per la gestione portuale e di sistemi ITS stradali sono ora **obbligati** a:

- **Garantire** un **approccio security by design**, ovvero che i **prodotti** siano progettati e sviluppati con requisiti di sicurezza cyber integrati fin dall'inizio.
- **Documentare e comunicare le vulnerabilità**.
- **Fornire aggiornamenti di sicurezza** per tutta la durata di vita ragionevole del prodotto.
- **Notificare le vulnerabilità attivamente sfruttate entro 24 ore** all'ENISA e alle autorità nazionali.

Inoltre, il CRA introduce una **classificazione dei prodotti in tre categorie in base al profilo di rischio**, con requisiti di compliance crescenti: prodotti standard, prodotti importanti di classe I e prodotti importanti di classe II. Molti **sistemi** impiegati nelle **infrastrutture di trasporto** rientrano nelle **categorie più elevate**, richiedendo **valutazioni di compliance** da parte di organismi notificati terzi, ponendo **sfide significative** per la **catena di fornitura del settore**, che dovrà adeguare i processi di sviluppo e certificazione dei prodotti.

DIRETTIVA CER (Critical Entities Resilience)

La CER completa il quadro normativo lavorando in **tandem con la NIS2**. Mentre la **NIS2** si concentra sulla **resilienza digitale** e sulla **sicurezza delle reti**, la **CER** affronta le **minacce fisiche alle infrastrutture critiche**: atti di sabotaggio, terrorismo, catastrofi naturali, emergenze sanitarie e rischi ibridi.
Per il **settore dei trasporti**, la CER identifica le **entità critiche attraverso un processo di mappatura nazionale** condotto da ogni Stato membro, che deve identificare i servizi essenziali forniti, le interdipendenze con altri settori, le misure di sicurezza fisica esistenti e le vulnerabilità potenziali. Le **entità identificate come critiche** sono tenute a effettuare la **valutazione del rischio**, implementare **misure di sicurezza fisica e organizzativa**, notificare gli **incidenti** con potenziale **impatto significativo** e partecipare a esercitazioni di preparazione.

REGOLAMENTO MACCHINE

Il **Regolamento Macchine (UE) 2023/1230** sarà applicabile a partire dal **20 gennaio 2027**, introduce per la prima volta **requisiti espliciti di cybersicurezza per le macchine** con implicazioni dirette e significative per il **settore dei trasporti**, dove numerose tipologie di attrezzature e sistemi rientrano nel campo di applicazione del regolamento.

L'**articolo 9** e l'**Allegato III** del Regolamento introducono **requisiti essenziali di salute e sicurezza,** ovvero, i **fabbricanti di macchine** che includono **sistemi di controllo connessi, interfacce di programmazione, funzioni di aggiornamento remoto o sistemi di diagnostica online** devono garantire che la **macchina sia protetta contro corruzioni accidentali o intenzionali** che possano compromettere la **sicurezza**.
Per il settore dei trasporti, le categorie di prodotti più impattate includono: i sistemi di movimentazione automatizzata nei porti e nelle aree logistiche (gru, AGV — Autonomous Guided Vehicles, nastri trasportatori connessi); le attrezzature ferroviarie di bordo e di terra con interfacce digitali; i sistemi di

gestione del traffico stradale con componenti programmabili; i veicoli industriali e le macchine da cantiere connesse utilizzate nella manutenzione delle infrastrutture di trasporto.
Il **Regolamento richiede** che questi prodotti siano accompagnati da una **dichiarazione di compliance UE** che attesti il rispetto dei **requisiti essenziali, inclusi quelli di cybersecurity**.

La **relazione** tra il **Regolamento Macchine** e il **CRA** richiede un'**analisi attenta**, poiché i perimetri di applicazione si sovrappongono parzialmente. In linea di principio, per i prodotti con elementi digitali che rientrano anche nel campo di applicazione del CRA, quest'ultimo prevale per gli aspetti di cybersicurezza del software, mentre il Regolamento Macchine rimane competente per gli aspetti di sicurezza fisica e per i rischi di sicurezza correlati ai componenti hardware meccanici.
Le **imprese del settore trasporti** che **acquistano o sviluppano tali sistemi** devono quindi assicurarsi che i **fornitori** dimostrino **compliance a entrambi i quadri normativi**.

AI ACT

L'AI Act entrerà progressivamente in vigore **entro il 2027** e nell'**Allegato III** elenca esplicitamente tra i **sistemi ad alto rischio** i **sistemi di IA** utilizzati per la **gestione e il funzionamento del traffico stradale, dei trasporti pubblici e delle infrastrutture di mobilità.** Per questi sistemi, gli **obblighi normativi** sono **particolarmente rigorosi** e includono: la gestione del rischio lungo tutto il ciclo di vita del sistema; la qualità dei dati di addestramento con requisiti di accuratezza, completezza e rappresentatività; la tenuta di una documentazione tecnica dettagliata; la conservazione dei log automatici per la tracciabilità; la trasparenza verso gli utenti; la supervisione umana con meccanismi di override; e standard elevati di accuratezza, robustezza e cybersicurezza.

I **veicoli autonomi** e i **sistemi di trasporto intelligenti (ITS)** ricadono interamente in questa categoria, richiedendo rigorose valutazioni di compliance prima dell'immissione sul mercato. Per gli sviluppatori e gli operatori di sistemi di controllo del traffico aereo, sistemi di gestione ferroviaria basati su IA, piattaforme di ottimizzazione portuale e sistemi di guida autonoma, l'AI Act impone l'obbligo di registrazione in una banca dati europea dedicata ai sistemi ad alto rischio

Il campo applicativo dell'AI Act nel settore trasporti va ben oltre la mobilità di passeggeri. L'uso dell'IA per la **pianificazione automatizzata** delle spedizioni, la **manutenzione predittiva dei veicoli** e delle **infrastrutture** e l'ottimizzazione dei **magazzini e dei terminal logistici** deve rispettare le nuove regole europee. Anche se queste applicazioni non ricadono nell'elenco esplicito dell'Allegato III, devono comunque essere valutate caso per caso per determinare il livello di rischio effettivo.

In particolare, i **sistemi di manutenzione predittiva OT** — che impiegano algoritmi di machine learning per anticipare i guasti nelle reti ferroviarie, negli impianti portuali o negli aeromobili — presentano una **doppia rilevanza normativa**: sono soggetti all'**AI Act** per la componente algoritmica e al **CRA** o al **Regolamento Macchine** per la componente **hardware/software integrata** nei sistemi di controllo fisici. La convergenza di questi quadri normativi richiede un'analisi di compliance integrata che molte organizzazioni del settore non hanno ancora condotto.

Inoltre, l'**AI Act** e la **NIS2 si influenzano reciprocamente** in modo significativo **per il settore dei trasporti**. Da un lato, i **sistemi di IA ad alto rischio devono essere robusti contro i cyberattacchi** — l'AI Act richiede esplicitamente che i sistemi siano progettati per resistere a tentativi di manipolazione dei dati (data poisoning), agli attacchi di evasione del modello e ad altre minacce specifiche dell'IA. Dall'altro, le **organizzazioni soggette alla NIS2** che impiegano **sistemi di IA nei loro processi critici** devono includere questi **sistemi nel perimetro della valutazione del rischio cyber, con attenzione specifica alle vulnerabilità proprie dell'IA**.

Un aspetto critico riguarda la **trasparenza** e la **spiegabilità** dei **sistemi di IA nei trasporti**: l'AI Act richiede che gli operatori di sistemi ad alto rischio siano in grado di **spiegare le decisioni del sistema**, il che è particolarmente rilevante quando l'IA prende decisioni operative su infrastrutture critiche (ad esempio, re-routing automatico del traffico ferroviario, gestione degli slot aeroportuali, ottimizzazione dei flussi portuali). In caso di incidente cyber che comprometta un sistema di IA, la possibilità di ricostruire

il processo decisionale del sistema è **essenziale per la risposta all'incidente e per le indagini successive**.

Il contesto italiano: recepimento NIS2 e sfide specifiche

L'Italia presenta un quadro composito: da un lato, il Paese ha compiuto progressi significativi nell'architettura istituzionale della cybersicurezza, con la creazione dell'**Agenzia per la Cybersicurezza Nazionale (ACN)** nel 2021 e l'elaborazione della **Strategia Nazionale di Cybersicurezza 2022-2026**. Dall'altro, il **tessuto produttivo e infrastrutturale del settore trasporti** presenta **vulnerabilità strutturali** legate alla frammentazione degli operatori, alla **prevalenza di PMI nella filiera logistica** e alla presenza di **sistemi legacy** in infrastrutture critiche quali **ferrovie e porti**.

Il 2025 ha segnato un punto di svolta negativo per il settore: il già citato aumento del 134,6% degli incidenti cyber nel segmento trasporti e logistica ha posto il tema al centro del dibattito industriale e istituzionale. I principali gestori di infrastrutture nazionali — **RFI (Rete Ferroviaria Italiana), ENAV (Ente Nazionale per l'Assistenza al Volo**), i principali **gestori aeroportuali** e le **Autorità di Sistema Portuale** — hanno **avviato o intensificato programmi di adeguamento alla NIS2**, spesso in collaborazione con l'ACN.

Tuttavia, permangono **criticità significative**. La filiera logistica italiana è caratterizzata da una **forte polverizzazione**: accanto ai grandi operatori infrastrutturali, operano migliaia di piccole e medie imprese di autotrasporto, spedizione e logistica che rientrano nell'ambito di applicazione della NIS2 (in quanto fornitori di entità essenziali) ma che spesso non dispongono delle risorse — umane, tecnologiche e finanziarie — necessarie per implementare i requisiti della direttiva. Tali imprese rappresentano **anelli deboli della catena di fornitura** e **potenziali vettori di attacco** verso i grandi operatori.

Ruolo di ACN e sfide istituzionali

L'**ACN** ha assunto il compito di **coordinare l'implementazione della NIS2** in Italia, stabilendo la piattaforma di registrazione degli operatori, le linee guida tecniche per la gestione del rischio e i meccanismi di notifica degli incidenti. Il **CSIRT Italia**, operativo 24/7, gestisce la **risposta agli incidenti di interesse nazionale** e mantiene relazioni di cooperazione con gli omologhi europei attraverso la rete CSIRTs.

Una sfida istituzionale rilevante riguarda il **coordinamento tra l'ACN e i ministeri di settore** — in primis il **Ministero delle Infrastrutture e dei Trasporti** — e le **autorità di regolazione specifiche** (ENAC per l'aviazione, ART per i trasporti, Autorità di sistema portuale). La NIS2 impone un'architettura di supervisione con autorità competenti settoriali che devono coordinarsi con l'ACN come autorità nazionale principale. Definire confini chiari di competenza e meccanismi di cooperazione efficaci è essenziale per evitare duplicazioni e lacune regolamentari.

Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)

Parallelamente alla NIS2, in Italia è operativo **dal 2019 il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)** che costituisce un sistema di misure volto ad **assicurare** un livello elevato di **sicurezza delle reti** e dei **sistemi informativi dei soggetti** — pubblici e privati — che svolgono **funzioni essenziali** per lo Stato o che erogano **servizi essenziali** il cui malfunzionamento potrebbe recare un pregiudizio alla sicurezza nazionale, alla difesa, alle attività militari o alle relazioni internazionali della Repubblica.
Il PNSC, aggiornato nel 2024, ha identificato il **settore dei trasporti come priorità di intervento per il 2025-2026**, con stanziamenti specifici per il rafforzamento delle capacità cyber delle infrastrutture critiche nazionali, poiché un attacco informatico ai loro sistemi potrebbe bloccare servizi essenziali per l'economia e la sicurezza nazionale. In concreto**, rientrano** tipicamente nel PSNC:

- **RFI (Rete Ferroviaria Italiana)** per i sistemi di gestione e controllo della rete ferroviaria nazionale.
- **ENAV (Ente Nazionale per l'Assistenza al Volo)** per i sistemi di controllo del traffico aereo.
- **Principali Autorità di Sistema Portuale** per i sistemi di gestione portuale strategici.
- **Gestori degli aeroporti di interesse nazionale**.
- **Operatori di sistemi di trasporto intelligenti (ITS)** con impatto su reti stradali di valenza nazionale.

La convergenza IT/OT: il cuore della vulnerabilità moderna

Il **settore dei trasporti** è oggi il paradigma per eccellenza del **sistema cyber-fisico** (*CPS — Cyber-Physical System*), dove la distinzione tra **Information Technology (IT) e Operational Technology (OT)** sta rapidamente scomparendo. Comprendere questa **convergenza** è essenziale per **progettare strategie di sicurezza efficaci.**

Per decenni, i **sistemi OT** — il segnalamento ferroviario, i sistemi di controllo del traffico aereo, i sistemi di gestione dei terminal portuali, i semafori intelligenti — hanno **operato in reti chiuse**, **isolate (air-gapped)** dalle **reti IT aziendali**. Tale **separazione fisica** era la principale **garanzia di sicurezza**. L'esigenza di efficienza operativa, manutenzione predittiva, ottimizzazione energetica e connettività in tempo reale ha progressivamente eliminato questo isolamento.

Il problema dei sistemi legacy

Oggi i **sistemi OT di controllo dei trasporti** sono **connessi a reti IP, a piattaforme cloud** per l'analisi dei dati **e a reti di terze parti** per la manutenzione remota. Tale **connettività** espone le **infrastrutture fisiche** ad **attacchi** che un tempo erano limitati al mondo digitale. Un criminale che accede alla rete IT aziendale di un gestore ferroviario attraverso una credenziale rubata di un dipendente che lavora da remoto può, attraverso movimenti laterali nella rete, raggiungere i sistemi OT di segnalamento — con conseguenze potenzialmente catastrofiche per la sicurezza fisica dei passeggeri.

Inoltre, una **sfida tecnica enorme** è rappresentata dagli **asset OT progettati** e **implementati decenni fa**, **privi** di qualsiasi concetto di **sicurezza informatica nativa**. Nel settore ferroviario, sistemi di segnalamento con cicli di vita di 30-40 anni coesistono con moderni sistemi digitali. Nel settore marittimo, apparati di navigazione e controllo delle navi risalenti agli anni '90 sono collegati a reti moderne. Nel settore aereo, sistemi di controllo del traffico aereo con architetture sviluppate negli anni '80 sono stati progressivamente estesi e connessi.

E' importante evidenziare che aggiornare o sostituire questi **sistemi legacy** è estremamente **complesso e costoso** per diverse ragioni: richiedono fermi operativi prolungati in settori dove la continuità del servizio è critica; i produttori originali possono non essere più attivi, rendendo difficile ottenere patch di sicurezza; le certificazioni di sicurezza funzionale (safety) devono essere riottenute dopo ogni modifica; e il costo di sostituzione può essere proibitivo per operatori con risorse limitate.
Di fatto, l'integrazione di **componenti moderne** (IoT, cloud) con questi **sistemi vecchi** crea **lacune di sicurezza** sfruttabili per interruzioni operative o sabotaggi.

Safety & security: due dimensioni inscindibili

Nel settore OT dei trasporti, la **priorità assoluta** è storicamente la **"safety"** (i.e. la sicurezza delle persone). I sistemi sono progettati con ridondanze, fail-safe e procedure operative che minimizzano il rischio di incidenti fisici. Tuttavia, la **cybersecurity** introduce una categoria di rischio qualitativamente diversa: le **minacce informatiche** sono **dinamiche, intenzionali, adattive** e possono **compromettere** direttamente l'**integrità fisica** dei **sistemi di controllo.**

Un attacco sofisticato a un sistema di segnalamento ferroviario non crea un "guasto" gestibile dalle procedure di sicurezza tradizionali: crea condizioni anomale che le procedure di *fail-safe* non sono progettate per gestire, potenzialmente causando incidenti fisici gravi. Ciò richiede un **ripensamento** dell'**approccio alla sicurezza:** non più due discipline separate (Safety come responsabilità degli ingegneri ferroviari, Security come responsabilità del reparto IT), ma un'**unica disciplina integrata** di **"Cyber-Safety" che consideri le interdipendenze tra le due dimensioni.**

Raccomandazioni strategiche per gli operatori di settore

Sulla base del panorama degli attacchi analizzato, del quadro normativo in evoluzione e delle specificità del settore dei trasporti, di seguito alcune raccomandazioni operative e strategiche, utili sia per i grandi operatori infrastrutturali sia per le PMI della filiera, con la consapevolezza che la resilienza cyber del settore è determinata dal suo anello più debole.

Inoltre, la **resilienza cyber** non è uno stato da raggiungere, ma un **processo dinamico da mantenere**. Il **settore dei trasporti** deve passare da una logica di "compliance come obiettivo" a una logica di "**resilienza come capacità organizzativa permanente**".

Governance & responsabilità

- **Elevare la cybersecurity a tema di board -** La **NIS2** — e per i soggetti nel perimetro, il **PSNC** — impone la responsabilità diretta del management: questo non è solo un obbligo normativo ma una necessità strategica. Il Consiglio di Amministrazione deve includere la cybersecurity nell'agenda regolare, approvare le politiche di gestione del rischio e destinare risorse adeguate. È opportuno nominare un CISO (Chief Information Security Officer) con accesso diretto al top management e, per le entità soggette al PSNC, un responsabile specifico per gli adempimenti del Perimetro e per le relazioni con il CVCN.
- **Integrare la cybersecurity nella gestione del rischio aziendale e nell'ERM** - La cyber resilienza non deve essere trattata come un progetto IT separato, ma come parte integrante del framework di Enterprise Risk Management. Questo significa quantificare i rischi cyber in termini finanziari (impatto economico atteso, costi di risposta e ripristino, esposizione sanzionatoria NIS2 fino al 2% del fatturato mondiale), integrare i rischi cyber nelle valutazioni di investimento e assicurare la coerenza tra politiche di sicurezza informatica e strategie di continuità operativa.
- **Adottare il Framework NIST come modello di governance dinamica**. Il **NIST Cybersecurity Framework** — nelle sue funzioni core Govern, Identify, Protect, Detect, Respond, Recover e la— offre un linguaggio comune e un modello strutturato per la gestione del rischio cyber adatto alla complessità del settore dei trasporti. Implementare questo framework consente di passare da una logica di semplice protezione a una governance ciclica e adattiva della sicurezza, integrando i requisiti NIS2, AI Act, CRA e PSNC in un unico sistema di gestione.
- **Definire chiare catene di responsabilità e procedure di escalation** - In caso di incidente, ogni ora persa in discussioni su "*chi fa cosa*" si traduce in danni operativi crescenti. Definire ex ante ruoli, responsabilità e procedure di comunicazione — interne (management, reparto IT/OT, legale, comunicazione) ed esterne (ACN/CSIRT, autorità di settore, partner, clienti) — è fondamentale per una risposta rapida ed efficace. Le scadenze NIS2 (notifica iniziale entro 24 ore) rendono questo piano non negoziabile.

Gestione del rischio e la sicurezza tecnica

- **Condurre le valutazioni del rischio integrate IT/OT, con estensione ai sistemi IA** - Le valutazioni del rischio cyber devono coprire l'intero ecosistema tecnologico, inclusi i sistemi OT di controllo fisico e — con l'entrata in applicazione dell'AI Act dal 2026 — i sistemi di IA impiegati in funzioni operative critiche. Per i sistemi OT legacy, è necessaria un'analisi specifica delle vulnerabilità e delle compensating controls applicabili senza interrompere il servizio.

- **Implementare la micro-segmentazione delle reti** - Isolare i sistemi OT critici attraverso segmentazione di rete rigorosa — con firewall industriali, zone demilitarizzate (DMZ) e controlli di accesso granulari — impedisce la propagazione laterale degli attacchi. Ricerche di settore indicano che questa tecnica può ridurre l'impatto dei data breach del 40%. Per i sistemi legacy non aggiornabili, la segmentazione rappresenta spesso l'unica misura di compensazione praticabile.
- **Adottare il paradigma cybersecurity-by-design in ogni nuovo progetto**. Integrare la sicurezza fin dalle fasi iniziali di progettazione di nuovi sistemi e nelle procedure di gara d'appalto è il principio cardine del CRA e del Regolamento Macchine. I requisiti di sicurezza cyber — inclusi quelli specifici per i sistemi IA previsti dall'AI Act — devono essere inclusi esplicitamente nei capitolati tecnici di qualsiasi acquisizione di sistemi ICT od OT per infrastrutture di trasporto, evitando il costoso e spesso inefficace retrofit della sicurezza su sistemi già progettati.
- **Adottare il modello Zero Trust e il monitoraggio continuo tramite SOC specializzati OT** - Il paradigma Zero Trust è particolarmente adatto al settore dei trasporti, caratterizzato da reti eterogenee, numerosi utenti terzi e accessi remoti. Ogni accesso a sistemi critici deve essere autenticato, autorizzato e monitorato, indipendentemente dalla posizione dell'utente. I SOC tradizionali non sono attrezzati per monitorare ambienti OT: è necessario dotarsi di SOC specializzati o di servizi *MDR (Managed Detection and Response)* con competenze specifiche sui protocolli industriali (*Modbus, DNP3, IEC 61850*).
- **Gestire proattivamente le vulnerabilità con SLA definiti** – Purtroppo, ad oggi, molti operatori impiegano oltre tre mesi per correggere le vulnerabilità note, mentre gli aggressori le sfruttano in pochi giorni. Pertanto, occorrono processi di *vulnerability management* strutturati con SLA di *remediation* differenziati per criticità, *compensating controls* per le vulnerabilità non patchabili nei sistemi legacy e *penetration test* periodici su entrambi i domini IT e OT.

Sicurezza della supply chain e gestione fornitori

- **Estendere i requisiti di sicurezza ai fornitori attraverso clausole contrattuali vincolanti** - La catena di fornitura è il vettore di attacco in più rapida crescita. Le entità NIS2 devono richiedere evidenza della compliance (certificazioni, rapporti di audit), effettuare le valutazioni del rischio cyber per i fornitori critici e prevedere il diritto di audit. Per i soggetti PSNC, le acquisizioni ICT devono rispettare il processo di notifica all'ACN e le eventuali prescrizioni del CVCN.
- **Mappare l'intera catena di fornitura, incluse le terze parti di secondo e terzo livello** - Il 79% delle aziende monitora meno della metà della propria supply chain per la cybersicurezza come già evidenziato. Pertanto, strumenti di *threat intelligence* e piattaforme di supply chain risk management possono automatizzare il monitoraggio della postura di sicurezza dei fornitori, generando alert quando un fornitore chiave registra un incidente o una vulnerabilità critica.
- **Diversificare i fornitori tecnologici per ridurre le dipendenze geopolitiche** -Per il settore marittimo e per le infrastrutture portuali in particolare, la dipendenza da fornitori extra-UE per tecnologie critiche rappresenta un rischio di sicurezza nazionale che il PSNC e il Golden Power cyber mirano esplicitamente ad affrontare. Le decisioni di procurement per sistemi critici devono incorporare valutazioni geopolitiche, privilegiando fornitori europei o di Paesi alleati.
- **Verificare, nel tempo, la futura compliance dei fornitori di sistemi IA all'AI Act -** Con l'entrata progressiva in applicazione dell'AI Act, i fornitori di sistemi di IA ad alto rischio per il settore trasporti dovranno altresì dimostrare la compliance al Regolamento, inclusa la registrazione nella banca dati europea. I contratti di fornitura dovranno prevedere clausole di compliance all'AI Act e il diritto di accesso alla documentazione tecnica richiesta dal Regolamento.

Preparazione operativa, risposta agli incidenti e business continuity

- **Sviluppare e testare piani di risposta agli incidenti specifici per il settore, con procedure separate per IT e OT.** I piani devono essere adattati alle specificità operative: la continuità del servizio è critica anche durante la gestione di un incidente; i sistemi OT richiedono procedure di risposta diverse dai sistemi IT; le implicazioni di safety devono essere integrate nelle

procedure di incident response. I piani devono essere testati regolarmente attraverso esercitazioni tabletop e simulazioni di incidente, con particolare attenzione agli scenari di attacco ai sistemi di controllo fisico.

- **Partecipare alle esercitazioni cyber a livello UE e nazionale.** ENISA organizza regolarmente esercitazioni settoriali; ERA ed ENISA organizzano esercitazioni specifiche per il ferroviario; EASA coordina quelle per l'aviazione. La partecipazione permette di testare le capacità di risposta in un ambiente sicuro e migliorare il coordinamento inter-organizzativo.
- **Predisporre piani di Business Continuity che contemplino il fallimento delle reti pubbliche**. Un attacco sofisticato può compromettere le reti di comunicazione ordinarie (4G/5G). I piani di continuità operativa devono prevedere canali alternativi — radio, linee dedicate, sistemi satellite — per garantire il coordinamento operativo e la comunicazione con le autorità anche durante una crisi cyber. Tale pianificazione deve coprire anche le interdipendenze con le reti energetiche e le telco, considerando scenari di crisi multi-settore.
- **Pianificare il ripristino considerando le interdipendenze interne IT/OT**. Una violazione di sistemi IT aziendali — email, sistemi di identità, infrastrutture di rete — può interrompere i sistemi OT anche se tecnicamente non compromessi. La pianificazione del disaster recovery deve essere olistica, identificando i punti di contatto critici tra IT e OT e i servizi condivisi la cui indisponibilità blocca l'intera organizzazione.

Competenze, cultura della sicurezza e compliance all'AI Act

- **Investire nella formazione continua e nella creazione di programmi di Cybersecurity Champions.** Per colmare il gap di competenze specifiche nel settore OT, è consigliabile selezionare e formare figure di *"Cybersecurity Champions*" all'interno del personale operativo esistente — ingegneri ferroviari, operatori portuali, tecnici aeroportuali. Tali profili, che combinano la conoscenza operativa con competenze di sicurezza informatica di base, possono fungere da prima linea di difesa e punto di contatto tra il reparto operativo e il team di cybersecurity, colmando il gap di competenze attraverso l'upskilling interno.
- **Formare il personale sui rischi specifici dell'IA e sulla supervisione umana dei sistemi.** L'AI Act impone la supervisione umana per i sistemi di IA ad alto rischio nei trasporti. Il personale che interagisce con questi sistemi deve essere formato non solo sul loro utilizzo operativo, ma anche sui rischi specifici dell'IA (data poisoning, allucinazioni algoritmiche, manipolazione dell'input) e sulle procedure di *override* da attivare quando il sistema produce output anomali o inattendibili, in particolare in scenari di possibile compromissione cyber.
- **Collaborare con ISAC e comunità di settore per la condivisione delle informazioni sulle minacce**. Aviation ISAC, EU Maritime ISAC, European CISO Forum for Rail e i ISAC nazionali coordinati dall'ACN sono le strutture di riferimento. La condivisione delle informazioni sulle minacce specifiche del settore è uno dei meccanismi più efficaci per migliorare la postura collettiva di sicurezza a costo contenuto.

Conclusione

Il **normativo europeo** - che comprende NIS2 Directive, AI Act, Cyber Resilience Act, CER Directive e il Regolamento Macchine - insieme al **Perimetro di Sicurezza Nazionale Cibernetica** (PNSC), delinea un'**architettura di resilienza** che sta ridefinendo in profondità il settore dei trasporti e che richiede il **passaggio** da una gestione reattiva della sicurezza **a un approccio proattivo**, **integrato e sistemico**.

Tale **architettura** non è solo **multilivello** sul piano normativo, ma anche **multidimensionale**: abbraccia la sicurezza delle reti, dei prodotti digitali, delle macchine connesse, dei sistemi di intelligenza artificiale e delle infrastrutture fisiche critiche. In particolare, per gli operatori strategici italiani, il **PSNC** introduce **requisiti rafforzati di controllo** e **protezione** lungo tutta la **supply chain ICT.**

Permangono, tuttavia, significative **differenze** nei livelli di **maturità** tra i diversi **sottosettori del trasporto** e colmare questi divari non rappresenta soltanto un **obbligo di compliance**, ma una

priorità strategica per la **sicurezza** economica e operativa dell'intero **sistema europeo**. La **vera sfida**, infatti, non risiede tanto nella definizione quanto nella **attuazione** delle **norme**: tradurre requisiti complessi in pratiche operative efficaci, in un contesto eterogeneo per dimensioni, competenze e risorse, richiede uno **sforzo coordinato e continuativo**.

Pertanto, il **successo** di questa trasformazione dipenderà dalla **capacità dell'ecosistema istituzionale** — incluse organizzazioni come ENISA e Agenzia per la Cybersicurezza Nazionale — di fornire **indirizzo**, **supporto** e **strumenti concreti**, nonché dal **ruolo attivo** delle **associazioni di settore** nella diffusione delle **best practice** e nello **sviluppo delle competenze**.

In ultima analisi, significa adottare una vera e propria **cultura della resilienza**, in cui la **sicurezza** diventa un **elemento centrale** nelle decisioni progettuali, operative e strategiche, sostenuta da **investimenti adeguati** e da una **governance** all'altezza della complessità delle minacce attuali e future per la sicurezza e la sostenibilità dei nostri ecosistemi.

Fonti e riferimenti

Il presente white paper si fonda su un'analisi integrata del quadro normativo europeo e nazionale, nonché su studi e report di riferimento elaborati dalle principali istituzioni e agenzie competenti in materia di cybersicurezza e resilienza delle infrastrutture critiche, con particolare attenzione al settore dei trasporti.

Normativa europea di riferimento

- Direttiva (UE) 2022/2555 – NIS2
- Regolamento (UE) 2024/2847 – Cyber Resilience Act (CRA)
- Regolamento (UE) 2024/1689 – AI Act

Normativa e contesto nazionale italiano

- Decreto Legislativo 4 settembre 2024, n. 138 – Recepimento Nis 2
- Perimetro di Sicurezza Nazionale Cibernetica (PSNC)

Report istituzionali e fonti di analisi

- ENISA Transport Threat Landscape (2023)
- ENISA NIS360 Report 2025