# Cybersecurity e sicurezza portuale, Paroli al 24° Forum Ict Security: «proteggere i porti significa difendere un nodo strategico del paese»

*19 Novembre 2026*




**Dalla minaccia cibernetica alla sorveglianza subacquea, l'AdSP rafforza gli investimenti in digitalizzazione e sicurezza, puntando sull'innovazione tecnologica e sulla collaborazione con le eccellenze industriali e accademiche italiane.**

Anche i porti civili sono diventati obiettivi strategici, esposti a minacce che possono assumere forme diverse, dalla dimensione cibernetica alle intrusioni fisiche e subacquee. È questo uno dei temi al centro dell'intervento del presidente dell'Autorità di Sistema Portuale del Mar Ligure Occidentale, Matteo Paroli, che il 19 novembre ha partecipato a Roma al panel «*Mediterraneo cyber: cavi sottomarini, hub portuali, kinetic spillover*», nell'ambito del 24° Forum ICT Security.

Il confronto, moderato dalla professoressa Paola Girdinio, presidente del Centro di Competenza START 4.0, ha riunito rappresentanti della Marina Militare, dell'Associazione Italiana Infrastrutture Critiche, di Elettra TLC e Prysmian per approfondire le interdipendenze tra infrastrutture digitali, collegamenti sottomarini e hub portuali, in uno scenario internazionale nel quale le tensioni geopolitiche possono produrre conseguenze dirette sulla sicurezza e sulla continuità dei servizi essenziali.

Nel suo intervento, Paroli ha richiamato innanzitutto un dato di contesto: la sicurezza degli scali non riguarda più soltanto le infrastrutture militari. Anche i porti commerciali e civili sono diventati bersagli potenziali, proprio per il ruolo che svolgono nell'approvvigionamento di beni essenziali all'economia dei Paesi.

Un esempio concreto è rappresentato dalla vicenda della petroliera Seajewel, danneggiata nella notte tra il 14 e il 15 febbraio 2025 da due esplosioni al largo di Vado Ligure, mentre scaricava greggio. Come ha ricordato il Presidente, la nave era stata attaccata con una mina magnetica applicata alla chiglia mentre attendeva l'ingresso in porto. La detonazione era stata in parte assorbita dal fasciame di rinforzo della struttura navale, evitando conseguenze più gravi. Un episodio che ha reso evidente come anche uno scalo civile possa essere esposto a minacce riconducibili a scenari di conflitto e a forme di aggressione non convenzionali.

Non occorre più difendere soltanto le acque dei porti militari come La Spezia o Taranto, ma anche i porti ordinari, i porti civili, che sono diventati bersagli attendibili, ha osservato Paroli sottolineando come la protezione degli scali debba necessariamente assumere una prospettiva integrata, capace di comprendere la dimensione digitale, quella terrestre, aerea e subacquea.

La crescente digitalizzazione dei processi logistici rende infatti i porti sempre più dipendenti dalla continuità dei sistemi informatici e delle reti di comunicazione. Oggi le merci viaggiano insieme ai dati: la gestione delle operazioni di carico e scarico, la pianificazione dei piani nave, il coordinamento dei terminal e lo scambio di informazioni tra amministrazioni e operatori sono attività strettamente interconnesse. Un attacco informatico riuscito può quindi produrre conseguenze che vanno ben oltre il perimetro dell'infrastruttura colpita, propagandosi lungo l'intera rete logistica e coinvolgendo il sistema produttivo nazionale.

Per affrontare queste nuove vulnerabilità, l'AdSP ha raddoppiato gli investimenti destinati alla digitalizzazione dei processi e al rafforzamento della cybersecurity, portandoli a oltre 6 milioni di euro. Un impegno che punta a sviluppare parallelamente l'efficienza dei sistemi informativi e la capacità di prevenire, individuare e contrastare le minacce informatiche, garantendo la continuità operativa degli scali. Accanto agli investimenti tecnologici, il Presidente ha richiamato anche la necessità di una protezione omogenea lungo tutta la filiera portuale, attraverso il coordinamento tra istituzioni, operatori e imprese, senza lasciare scoperte le realtà di minori dimensioni.

Sul fronte della sicurezza fisica e del monitoraggio, l'Autorità sta sviluppando un programma di innovazione che coinvolge anche eccellenze industriali e accademiche nazionali, tra cui Fincantieri e il Politecnico di Milano, per potenziare le capacità di sorveglianza e controllo degli ambiti portuali attraverso sistemi a pilotaggio remoto e tecnologie avanzate.

In particolare, il progetto dei droni automatizzati Drone in a Box prevede a regime l'installazione di tredici stazioni autonome di decollo, atterraggio e ricarica, con altrettanti velivoli professionali equipaggiati con telecamere ad alta risoluzione e sensori termici. Il sistema consentirà di programmare missioni di monitoraggio e sorveglianza, supportare le attività di security e safety, verificare lo stato delle infrastrutture e intervenire con maggiore tempestività nelle situazioni di emergenza.

A questa componente si affianca la collaborazione con Fincantieri per lo sviluppo di sistemi di protezione delle acque portuali, basati sull'integrazione di sensori acustici, boe, sonar e droni subacquei autonomi, capaci di rilevare eventuali intrusioni e individuare situazioni anomale anche in ambienti nei quali la videosorveglianza tradizionale non è efficace. L'obiettivo è costruire un sistema di monitoraggio progressivamente integrato, esteso dalla superficie del mare alle infrastrutture sommerse.

Accanto agli investimenti tecnologici, ha proseguito il Presidente Paroli, è indispensabile puntare sulle competenze e sulla formazione delle persone. Il fattore umano rappresenta infatti una componente essenziale di qualsiasi sistema di difesa: anche le infrastrutture più sofisticate possono rivelarsi vulnerabili se chi opera all’interno dell’organizzazione non è adeguatamente preparato a riconoscere e gestire le minacce. La sicurezza si costruisce affiancando alle barriere tecnologiche una cultura condivisa della prevenzione, capace di coinvolgere tutto il personale e l’intera filiera logistico-portuale.

«*La sicurezza di un porto non può essere affrontata guardando a una sola dimensione. Dobbiamo proteggere le infrastrutture fisiche, i sistemi digitali, le reti di comunicazione e gli specchi acquei, mettendo a sistema competenze pubbliche, industriali e tecnologiche*», è il principio che ha guidato l'intervento del Presidente.

La sfida, in definitiva, non riguarda soltanto la protezione dei singoli scali, ma la salvaguardia di una rete di connessioni dalla quale dipendono la competitività delle imprese, la continuità delle attività produttive e la sicurezza degli approvvigionamenti del Paese.