Paroli addresses the 24th ICT SECURITY FORUM: “Protecting ports means safeguarding a strategic national asset”

19 November 2026



From cyberthreats to underwater surveillance, the Western Ligurian Sea Port Authority is stepping up investment in digitalisation and security, focusing on technological innovation and cooperation with leading Italian industrial and academic institutions.

Commercial ports have increasingly become strategic targets, exposed to a growing range of threats, from cyberattacks to physical and underwater incursions. This was one of the key themes addressed by Matteo Paroli, President of the Western Ligurian Sea Port Authority, in the panel discussion entitled “Cyber Mediterranean: Undersea Cables, Port Hubs and Kinetic Spillover”, at the 24th edition of the ICT Security Forum held in Rome on 19 November 2026.

The event grouped together senior representatives from the Italian Navy, the Italian Association for Critical Infrastructure, Elettra TLC and Prysmian to examine interaction between digital infrastructure, undersea communication links and port hubs, against a backdrop of international geopolitical tensions with potentially direct implications for security and the seamless provision of essential services.

In his address, Paroli highlighted a fundamental shift in security management: the safeguarding of ports can no longer be an issue confined to military infrastructure alone. Commercial ports, too, are potential targets, given their strategic role in ensuring the supply of goods that are essential to the economy of the nation. “We can no longer focus solely on protecting the waters surrounding military ports, such as La Spezia and Taranto. Commercial and passenger ports have also become potential targets,” remarked Matteo Paroli stressing the need for an integrated approach to port security, encompassing digital, land, air and underwater domains.

The increasing digitalisation of logistic processes contributes to a growing dependence of the ports on the reliability and continuity of IT systems and communication networks. Today, goods move alongside data: cargo handling operations, vessel stowage planning, terminal coordination and data exchange between public authorities and private operators are all closely interconnected. A successful cyberattack can, therefore, have consequences extending far beyond the boundaries of the infrastructure directly affected, potentially disrupting the wider logistics network and impacting the national supply chain.

To address these emerging vulnerabilities, the Port Authority has doubled its investment in digitalisation and cybersecurity, exceeding a total of €6 million. The programme is designed to

strengthen the resilience of IT systems and enhance the capacity to prevent, detect and counter cyber threats, while safeguarding the operational continuity of port activities.

Alongside these investments, the Port Authority is pursuing an extensive technological innovation programme, in cooperation with leading Italian industrial and academic partners, including Fincantieri and the Politecnico University of Milan, to enhance surveillance and monitoring capabilities across port areas through the deployment of unmanned systems and other advanced technologies.

A key component of this programme is the Drone in a Box project, which envisages the installation of thirteen autonomous take-off, landing and recharging stations, each equipped with a professional-grade drone featuring high-resolution cameras and thermal sensors. The system is designed to carry out pre-programmed surveillance and monitoring missions, support security and safety operations, assess infrastructure conditions and ensure a more rapid response in emergency situations. This initiative is complemented by a new partnership with Fincantieri to develop advanced IT systems to protect port waters. These will integrate acoustic sensors, buoys, sonar equipment and autonomous underwater vehicles to detect potential intrusions and identify anomalies, including in areas beyond the reach of conventional video surveillance. The objective is to establish an increasingly integrated monitoring system, extending from the sea surface to underwater infrastructure.

Alongside technological investment, President Paroli emphasised the importance of developing specialist skills and providing appropriate training. The human factor remains a crucial component of any security framework: even the most sophisticated infrastructure can prove vulnerable if those working within an organisation are not adequately equipped to recognise and respond to potential threats. Effective security, therefore, requires technological safeguards, bolstered by a shared vision and a coordinated commitment involving the entire workforce and the wider port and logistics supply chain.

“Port security cannot be addressed from a single perspective. We must protect tangible infrastructure, digital systems, telecommunication networks and port waters, bringing together the public administrations, industry and technological expertise,” concluded President Paroli.