# Without cybersecurity there are no Smart Ports

Rafael Company Peris

Security

*Cybersecurity, Smart Ports, Digital port transformation, NIS2 Directive*

*Every day, thousands of vessels connect ports around the world, carrying more than 80% of international trade by volume. Behind every port call lies a complex network of digital systems that coordinates vessel arrival, berth allocation, operations planning, container movement, customs controls and the inland transport of goods, among other tasks. What only two decades ago depended mainly on physical infrastructure and coordination between people is now supported by digital platforms, IoT sensors, artificial intelligence, communications networks and automation systems.*

This transformation has turned ports into true **cyber-physical ecosystems**. The efficiency gained through **digitalization** has made it possible to reduce port-call times, optimize resources and improve cargo traceability. However, it has also generated a growing technological dependence that widens the exposure surface to **cyberthreats** that are increasingly sophisticated.

**Cyberattacks** no longer affect only computers or databases. They can paralyze terminals, disrupt logistics operations, compromise industrial systems or disrupt services that are essential for international trade. In an environment where the availability of information is as important as the availability of physical infrastructure, **cybersecurity** has ceased to be a technical function and has become a **strategic element of port management**.

The European Union has responded to this evolution through a set of initiatives that strengthen the protection of critical infrastructure, most notably the **NIS2 Directive**, the **Critical Entities Resilience Directive (CER),** the **Cyber Resilience Act** and the **Artificial Intelligence Act**. All of them reflect the same reality: the security of the European port system increasingly depends on its ability to anticipate, withstand and recover from incidents that combine **physical** and **digital dimensions**.

This article analyzes how digital transformation is redefining **cybersecurity in European ports,** what the main threats facing the sector are, and why protecting cyberspace has become an essential requirement for ensuring the continuity of critical infrastructure on which a large part of the world economy depends.

## The digital revolution of ports

For centuries, the **competitiveness of a port** was determined by physical factors such as the depth of its basins, the length of its quays, its storage capacity or the quality of its inland connections. Although these elements remain essential, digital transformation has added a new component that is equally decisive: the ability to **manage information quickly**, **securely** and **efficiently**.

**Modern ports** are no longer merely places where goods are transferred between maritime and land transport. They are **highly connected logistics platforms** where shipping lines, terminals, port authorities, shipping agents, rail operators, customs, security forces and a broad ecosystem of technology providers all converge. Coordination among all of them depends, to a large extent, on **digital systems** that make it possible to exchange information in real time and optimize decision-making.

The evolution toward the **Smart Port** concept has accelerated this process. Technologies such as the Internet of Things (IoT), artificial intelligence, big data analytics, private 5G networks, digital twins and cloud computing are transforming the way port operations are managed. **Distributed sensors** monitor the condition of critical infrastructure, **algorithms** optimize internal traffic, **digital platforms** facilitate logistics

coordination, and **intelligent systems** make it possible to anticipate incidents before they affect operations.

Another key element in this transformation has been the consolidation of **Port Community Systems (PCS)**, platforms that facilitate the secure exchange of information among the different actors in the port community. Thanks to these systems, documents that were traditionally handled on paper have been replaced by digital processes that reduce administrative times, improve traceability and increase operational efficiency.

At the same time, **terminal automation** has driven the incorporation of connected equipment capable of operating with a high degree of autonomy. Automated cranes, automated guided vehicles (AGVs), industrial control systems and predictive maintenance solutions **increase productivity** and **reduce operating costs**. However, this evolution also entails a growing interdependence between **information technologies (IT)** and **operational technologies (OT),** traditionally managed independently.

This convergence is one of the greatest challenges in port cybersecurity. While **IT systems** were designed to manage corporate information, **OT systems** control physical processes whose availability is critical to the continuity of operations. The connection between both environments brings significant benefits, but it also creates new access routes that can be exploited by malicious actors.

Digitalization has also increased dependence on **external software providers**, **cloud services** and **connected devices**. Each new technological integration brings operational advantages, but it also introduces new risks associated with vulnerabilities, configuration errors or compromises in the digital supply chain. Port security therefore no longer depends solely on its own systems but is instead shaped by a much broader **technological ecosystem** .

This changing landscape forces a rethink of the traditional concept of security. Protecting the physical perimeter of facilities is no longer enough. The true **border of a smart port** now extends to communications networks, digital platforms, sensors, mobile devices and distributed services that operate both inside and outside the port precinct.

As a result, **cybersecurity** is no longer understood as a technological support function but has become an **essential element of operational continuity**. The availability of a port management system, the integrity of data exchanged between operators, or the protection of an industrial network can today have as decisive an impact on port activity as the operation of a crane or the availability of a berth.

The evolution toward increasingly smart ports is not only transforming the way they operate. It is also redefining the very concept of security. Understanding this new reality is the first step toward facing an environment in which threats no longer distinguish between the physical and digital worlds.

## The new map of cyberthreats: when digital risk becomes operational risk

**Digitalization** has profoundly transformed port activity, but it has also changed the nature of the threats the sector faces. If barely a decade ago the main concern was protecting corporate information from theft or data loss, today the **target of a cyberattack** can be far more ambitious: disrupting a terminal's activity, compromising an industrial system, altering the logistics chain, or affecting the supply of essential services.

This evolution largely reflects the growing **strategic value of ports**. As key nodes of international trade and supply chains, ports concentrate a large volume of goods, critical infrastructure, sensitive information and services whose disruption can generate major economic and social consequences. For a cybercriminal, an organized criminal group or even a state-sponsored actor, a port represents a high-impact target.

In addition, the **motivation behind attacks** has changed. While incidents focused on information theft used to predominate in the past, campaigns aimed at **paralyzing operations**, **extorting money** from organizations, or **destabilizing strategic infrastructure** are now widespread. The line between cybercrime, industrial espionage and hybrid threats is becoming increasingly blurred.

## From ransomware to operational sabotage

**Ransomware** remains one of the main threats to the maritime-port sector. This type of attack encrypts an organization's information and **blocks access to critical systems** until a ransom is paid. However, its impact goes far beyond data loss.

In a **highly digitalized port**, the unavailability of document management platforms, terminal planning systems or logistics applications can cause operational delays, congestion at access points, difficulties coordinating the movement of goods, and significant financial losses for all actors in the port community.

One of the best-known examples was the **NotPetya** attack suffered by **Maersk** in 2017. Although the company was not the initial target of the **malware**, the infection spread rapidly through its corporate network and affected hundreds of applications and thousands of servers worldwide. Recovery required weeks of work and resulted in estimated losses of hundreds of millions of dollars. Beyond the economic impact, the incident showed just how far a large logistics organization could be brought to a virtual standstill by a cyberattack.

More recent cases, such as the incidents suffered by **DP World Australia** in 2023 or the **Port of Nagoya** that same year, confirm that these threats continue to evolve. In both cases, port operations experienced **significant disruptions** that affected the movement of goods and forced the activation of contingency procedures to restore operations.

These episodes show that cybersecurity can no longer be measured solely by the number of compromised systems or the volume of information affected. Its true impact must be assessed based on the consequences for **operational continuity**.

## The digital supply chain: the weakest link

The growing **interconnection** between organizations has made the digital supply chain one of the main risk vectors.

A port maintains permanent connections with shipping lines, terminals, freight forwarders, customs authorities, software providers, maintenance companies, logistics operators and numerous external services. Each of these relationships involves the **exchange of information** and, in many cases, the **interconnection of systems**.

This reality creates a scenario in which the **security of the whole** depends on the level of protection of the most vulnerable link.

Attacks targeting **technology providers** have multiplied in recent years because they make it possible to compromise multiple organizations simultaneously using a single point of access. This type of threat requires broadening the traditional view of cybersecurity. It is no longer enough to protect one's own infrastructure; it is essential to assess **third-party risk**, establish security requirements for suppliers, and continuously monitor the trust relationships that exist within the digital ecosystem.

## The convergence of IT and OT: a new attack surface

Another feature that defines the evolution of threats is the growing interest in **industrial systems**.

For many years, **operational technologies (OT)** remained isolated from corporate networks and, as a result, had limited exposure to cyberattacks. However, the digitalization of operations has fostered a progressive integration between **IT** and **OT environments** to improve efficiency, facilitate remote maintenance and optimize asset management.

Although this convergence brings significant operational benefits, it also significantly increases the **attack surface**.

Automated cranes, access control systems, power grids, energy supply stations, fuel facilities and communications infrastructure are all part of an environment in which a **cyber incident** can have immediate physical consequences. Manipulating these systems not only compromises information but can also directly affect the safety of people and the continuity of operations.

This reality calls for **specific protection strategies** for **OT environments**, different from those traditionally applied to corporate networks.

## New threats for a connected port

The risk landscape continues to expand with the incorporation of new technologies.

The use of satellite navigation and positioning systems has heightened concern over **jamming** and **spoofing** attacks, capable of altering the positioning information used by vessels and certain port services.

Likewise, the growing use of **artificial intelligence** poses a **double challenge**. On one hand, it offers advanced capabilities for detecting anomalies, identifying behavioral patterns and improving incident response. On the other, it makes it easier for attackers to automate phishing campaigns, develop malicious code more quickly, or generate fake content that is increasingly difficult to identify.

**Hybrid threats** add another dimension to this scenario. The combination of cyberattacks with disinformation campaigns, physical sabotage or geopolitical pressure highlights that port protection goes beyond the strict technological realm and is part of the European Union's economic and strategic security.

## A matter of operational continuity

All these examples point to the same conclusion: the main risk no longer lies solely in suffering a cyberattack, but in the **ability to keep operating** when one occurs.

Experience shows that no organization can guarantee **absolute protection** against a constantly evolving threat landscape. That is why the real **challenge** lies in reducing the likelihood of a successful attack, detecting incidents early, responding quickly and restoring operations with the least possible impact.

This shift in perspective explains why **cybersecurity** has become a priority in critical infrastructure management strategies. The issue is no longer just protecting IT systems but ensuring the continuous operation of essential services that underpin a large part of international trade.

## Europe responds: a new framework to protect critical infrastructure

The growing digitalization of ports and the rise in cyberthreats have led the **European Union** to rethink its **strategy for protecting critical infrastructure**. Cybersecurity can no longer be addressed solely from a technological perspective; it requires a comprehensive approach that combines governance, risk management, cooperation and operational continuity.

In this context, the **NIS2 Directive**, adopted in 2022, replaces the earlier NIS Directive and significantly broadens its scope. Beyond introducing new regulatory obligations, NIS2 represents a paradigm shift: cybersecurity becomes a strategic responsibility of the organization as a whole, not just of its technology departments.

For port authorities, terminals and other operators considered essential or important entities, the directive requires the implementation of risk management measures, strengthening of supply chain security, establishment of incident notification procedures, development of continuity plans, and ensuring that senior management is involved in cybersecurity-related decision-making.

However, NIS2 does not operate in isolation. It is part of a broader regulatory ecosystem that includes the **Critical Entities Resilience Directive (CER)**, aimed at strengthening protection against physical and technological risks; the **Cyber Resilience Act (CRA)**, which establishes cybersecurity requirements for products with digital components; and the **European Artificial Intelligence Regulation (AI Act)**, which introduces specific obligations for high-risk AI systems.

The **common goal** of these initiatives is to strengthen European strategic autonomy and ensure that critical infrastructure can continue to provide essential services even in scenarios of high technological or geopolitical pressure.

For the port sector, this framework represents an **opportunity** to move toward management models in which **cybersecurity** is integrated into strategic planning, business continuity and overall risk management.

## The cybersecurity of the smart port

The evolution of threats also requires rethinking how a port is protected. Traditional strategies, based on perimeter protection and the separation between information technologies (IT) and operational technologies (OT), are **insufficient** to respond to a **highly interconnected environment**.

The smart port requires an integrated approach to cybersecurity. This means applying principles such as network segmentation, robust authentication, continuous monitoring, vulnerability management, and the exchange of threat intelligence. Models such as **Zero Trust**, which start from the premise that no user or device should be considered trustworthy by default, are gradually being incorporated into the security architectures of critical infrastructure.

The **protection of OT systems** is another of the **major challenges**. Unlike IT environments, where software updates and patching are part of routine operations, many industrial systems must prioritize service availability and have much longer life cycles. This calls for the development of specific protection strategies that balance security with operational continuity.

**Artificial intelligence** is also changing the way cybersecurity is managed. Its ability to analyze large volumes of information facilitates the early detection of anomalies, the correlation of events and the identification of suspicious behavior. However, these same capabilities can be used by malicious actors to automate attacks or develop increasingly sophisticated social engineering campaigns, which require maintaining human oversight and continuously assessing the risks associated with these technologies.

Alongside technological solutions, the **human factor** remains one of the most important elements of cybersecurity. Staff training, incident response exercises, coordination between organizations and the development of a security culture are measures just as important as the deployment of new tools. Experience shows that the ability to detect and manage an incident depends as much on people and processes as it does on available technology.

Ultimately, the cybersecurity of the smart port is not built solely on firewalls or intrusion detection systems. It rests on **a balanced combination of technology**, **governance**, **cooperation** and **preparedness** to respond to increasingly complex incidents.

## Conclusions

**Digital transformation** has turned ports into one of the best examples of **critical cyber-physical infrastructure**. The adoption of advanced technologies has increased the sector's efficiency and competitiveness, but it has also broadened the exposure surface to threats that evolve very rapidly.

In this scenario, cybersecurity ceases to be a technological requirement and becomes an **essential component of port management**. Protecting networks, industrial systems and digital platforms means protecting the continuity of operations, the trust of the port community, and the stability of the logistics chains on which a large part of international trade depends.

The **European response,** embodied in initiatives such as **NIS2**, **CER**, **CRA** or the **AI Act**, reflects an increasingly integrated vision of critical infrastructure protection. The goal is no longer merely to prevent incidents, but to build organizations capable of anticipating, responding to and recovering quickly from them.

For European ports, this shift represents much more than a **regulatory challenge**. It is an opportunity to strengthen their competitiveness, build the trust of operators and customers, and move toward a management model in which security is part of the value they offer to the entire logistics chain.

For decades, a port's strength was measured by the capacity of its physical infrastructure and the efficiency of its operations. In the **digital economy**, that strength will also depend on its ability to **protect the cyberspace** that underpins those operations. Cybersecurity has ceased to be a support element and has become one of the **pillars of competitiveness**, **resilience** and the **sustainability** of the European port system.

## References

European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*.

European Commission. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)*.

European Commission. *Directive (EU) 2022/2557 on the resilience of critical entities (CER)*.

European Commission. *Cyber Resilience Act* (Regulation (EU) 2024/2847).

European Commission. *Artificial Intelligence Act* (Regulation (EU) 2024/1689).

International Maritime Organization (IMO). *Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2)*.

United Nations Conference on Trade and Development (UNCTAD). *Review of Maritime Transport 2024*.

European Maritime Safety Agency (EMSA). *Maritime Cybersecurity Best Practices*.

European Sea Ports Organisation (ESPO). *ESPO Environmental Report and Digitalisation Papers*.

World Economic Forum. *Global Cybersecurity Outlook*.

Pharos 39.0

Valenciaport Knowledge Hub

www.pharos390.com
info@pharos390.com