TECHNIUM
SOCIAL SCIENCES JOURNAL

# Vol. 79/2026

## A New Decade for Social Changes

PLUS COMMUNICATION
International Communication & PR

TECHNIUM SOCIAL SCIENCES JOURNAL

*Technium Social Sciences Journal*
*Vol. 79, 204-212, January, 2026*
*ISSN: 2668-7798*
*www.techniumscience.com*

# Europe's Port Achilles' Heel

**Gilles A. Paché**

CERGAM Lab, Aix-Marseille University, France

gilles.a.pache@gmail.com

**Abstract**. For several years, the growing vulnerabilities of European ports have become increasingly evident, revealing how exposed critical infrastructures are to simultaneous cyber, geopolitical, and organizational risks. The rapid digitization of port operations, coupled with the deep interconnection of global supply chains, has heightened the dependence of freight flows on complex IT systems, in which even minor failures can trigger major disruptions. As a result, ports are becoming high-value targets for actors seeking either to destabilize commercial activity or exploit structural weaknesses. This research note highlights the convergence of several issues: extreme process optimization that undermines system resilience, increasing reliance on heterogeneous technologies, and persistent difficulties in coordinating multiple public and private stakeholders. At the same time, the European Union (EU) faces strategic constraints due to the absence of a unified logistical vision and stark disparities in modernization between major gateways and secondary ports. In response, four priority areas of action emerge: integrating logistical policy into the broader EU industrial strategy, accelerating the digital transformation of port infrastructure, reinforcing cybersecurity and civil-military cooperation mechanisms, and harmonizing operational standards to enhance the overall resilience of the European port system.

**Keywords**. Cybersecurity, digitalization, European ports, logistics, maritime governance, risk management, supply chain vulnerabilities.

## 1. Introduction

In September 2025, the Western Ligurian Sea Port Authority, responsible for the Italian ports of Genoa, Prà, and Savona, experienced a cyberattack during the Genoa Boat Show; to mitigate risks and protect critical infrastructure, IT systems were temporarily shut down, paralyzing multiple terminals and disrupting operations including cargo unloading, dock scheduling, and port management [1]. Although the incident lasted only approximately two hours, it revealed the inherent vulnerability of European ports to digital threats, demonstrating that even major Mediterranean ports are susceptible and that physical and digital infrastructures are inseparably linked, where a single cyberattack can simultaneously halt cranes, docks, and terminals. The Italian case exemplifies a broader structural fragility: European ports function as essential nodes in global logistical networks, with disruptions potentially generating cascading effects across international trade flows. Since 2022, ports in Germany, the Netherlands, and Belgium have also been targeted by attacks that compromised energy supplies and disorganized maritime freight for several days [2]; the proliferation of

Technium Social Sciences Journal
Vol. 79, 204-212, January, 2026
ISSN: 2668-7798
www.techniumscience.com

such incidents highlights systemic risks that extend beyond individual terminals, emphasizing the strategic necessity of resilient port infrastructures for economic sovereignty, market continuity, and the stability of export-dependent industries.

The recurring exposure of European ports to cyber and operational risks parallels analyses of semiconductor supply chains, where fragility stems less from short-term shocks, which can often be absorbed, than from deeply embedded structural vulnerabilities within complex networks [3]. In logistics, as in semiconductor production, decision-makers have historically prioritized cost efficiency over resilience, resulting in hyper-optimized but rigid systems that lack redundancy and fail to absorb unforeseen shocks. European ports have similarly developed high-performing, technologically advanced systems that remain insufficiently robust; the COVID-19 pandemic demonstrated how minor disruptions can cascade into widespread operational delays. Modern ports function as integrated platforms combining automated terminals, advanced IT infrastructures, and massive streams of international data; the growing interconnectivity amplifies exposure to technical, climatic, economic, and strategic risks. Vulnerability is therefore not merely local, affecting a single terminal, but continental, with failures capable of propagating throughout thousands of global supply chains. The lack of a comprehensive EU strategy to safeguard this critical infrastructure compromises the continent's ability to maintain industrial sovereignty and ensure uninterrupted trade flows, leaving Europe dependent on external actors and increasingly exposed to global disruptions.

Digitization and automation have improved operational efficiency across European ports; however, these advancements simultaneously increase systemic exposure to cyberattacks and operational failures. Automated cranes, digital terminal planning, and predictive maintenance rely heavily on interoperable IT systems, and any disruption—whether malicious or technical—can halt port activity for extended periods, triggering cascading consequences along connected supply chains. Disparities between highly modernized hubs such as Rotterdam and Hamburg and less automated Mediterranean or Eastern European ports exacerbate this vulnerability; uneven adoption of smart technologies limits coordination, reduces throughput efficiency, and creates weak points that threaten overall resilience [2]. Effective risk mitigation requires a combination of technological modernization, standardized operational protocols, and coordinated governance structures across EU member States. Moreover, ports are no longer isolated operational units but complex nodes in global trade networks; disruptions in one location can influence supply chains across multiple sectors, including pharmaceuticals, electronics, and energy. Recognizing this, EU policymakers face the urgent challenge of embedding resilience into digital infrastructures while balancing efficiency and security, ensuring that modernization does not unintentionally amplify structural weaknesses and systemic risk.

Beyond technological and operational challenges, structural fragmentation within European logistics governance significantly undermines port resilience. Each EU member State manages its port infrastructure independently, resulting in disparate standards, incompatible information systems, and uncoordinated investment strategies; competition among neighboring ports further inhibits the development of integrated approaches to modernization, automation, and cybersecurity [2]. Without a unified EU framework, local disruptions—whether caused by cyberattacks, extreme weather, or labor conflicts—can escalate into continent-wide supply chain failures. Strategic coordination is therefore essential, encompassing shared protocols, centralized monitoring, and mechanisms for rapid

*Technium Social Sciences Journal*
*Vol. 79, 204-212, January, 2026*
*ISSN: 2668-7798*
*www.techniumscience.com*

intervention; harmonized cybersecurity standards and civil-military cooperation can strengthen preparedness against systemic threats. Additionally, targeted investment in undermodernized ports and the diffusion of smart technologies across all hubs would enhance interoperability and reduce structural inequities, creating a more robust continental network. In combination, these measures could secure Europe's industrial sovereignty, safeguard critical trade routes, and transform ports into resilient platforms capable of absorbing shocks while maintaining continuity of commerce and supply chain reliability under complex geopolitical and environmental pressures.

## 2. Europe's Maritime Gateways Under Foreign Grip

Since the Middle Ages, European ports have served as central engines of economic growth and strategic power, embodying a concept that can be described as "*logistical sovereignty*." Ports such as Rotterdam, Hamburg, Antwerp, Marseille, and Le Havre were critical nodes in intra-EU trade and maritime commerce with overseas colonies, facilitating the movement of raw materials, manufactured goods, and essential foodstuffs. Rotterdam, active since the 12th century as a river port, gradually emerged as the primary hub of Northwest Europe, with the 19th-century opening of the Nieuwe Waterweg canal linking the Rhine and Meuse rivers to the North Sea. This infrastructure allowed larger vessels to navigate efficiently and expanded the port's hinterland to encompass the Netherlands, Germany, Belgium, and beyond [4]. By the 1980s, the ten largest European ports concentrated approximately 60% of the continent's international container trade, with Rotterdam alone accounting for nearly 10% of European port activity [5]. These ports enabled nations to assert control over trade flows, monitor logistics effectively, and maintain industrial and economic security without relying directly on foreign powers, demonstrating the historical strategic value of concentrated maritime infrastructure.

Over the past three decades, the privileged position of European ports has been gradually challenged by global economic and geopolitical transformations. The expansion of international markets, the increasing role of non-EU actors, and the dynamics of globalization have created unprecedented pressures on a model that has long dominated EU trade. Since the 2000s, China has strategically integrated its industrial objectives into maritime infrastructure investments in Europe. COSCO Shipping Ports, a State-owned entity, has emerged as a major player both in Northern Europe and the Mediterranean, exemplified by its majority stake in the port of Piraeus acquired in 2009. Progressive expansion across almost all terminals has transformed the port into a major hub of the Belt and Road Initiative, linking Asia, the Middle East, and Europe, with container traffic increasing from 1.5 million TEUs in 2010 to over 5 million TEUs in 2023 [6]. Concurrently, Rotterdam, Hamburg, and Antwerp have granted minority stakes or concessions to foreign operators, often Chinese, allowing access to critical logistical operations and sensitive data. According to a European Commission report, these developments are closely monitored by the United States, reflecting concern over Beijing's growing influence in key EU hubs [7].

The influence of foreign actors in European ports is not solely an economic concern but also a critical geopolitical challenge, particularly given the strategic location of major hubs. Rotterdam, situated at the confluence of the Rhine and Meuse rivers, remains the primary gateway to Northwest Europe, handling 159 million tons in 2023, nearly 10% of the EU total [8]. Beyond geographic significance, the concentration of flows on a limited number of strategic ports amplifies Europe's vulnerability, as controlling these points provides access to

Technium Social Sciences Journal
Vol. 79, 204-212, January, 2026
ISSN: 2668-7798
www.techniumscience.com

extensive global supply chains. Recent crises—the war in Ukraine, the Suez Canal blockades, and the COVID-19 pandemic—have demonstrated the susceptibility of European ports to external shocks and reinforced the need for stronger EU oversight. Decades of investment and ambitious port policies have made logistical sovereignty a pillar of geoeconomic security. Yet Europe's fragility is not solely attributable to Chinese expansion: structural weaknesses within the continent's internal logistical frameworks further compromise resilience, leaving its entire network exposed to operational, cyber, and strategic disruptions.

EU logistical vulnerabilities are also linked to internal limitations in the coordination, security, and modernization of supply chains. The growing reliance on digital infrastructure exposes ports to cyber threats capable of paralyzing entire terminals. Research on digital risk management and the analysis of institutional cooperation around *Computer Security Incident Response Teams* (CSIRTs) emphasize that only close collaboration between ministries, public agencies, and private actors can bolster the resilience of critical systems [9]. Beyond cyber concerns, efficiency in maritime transport remains a decisive factor for EU competitiveness, reflecting the enduring importance of major infrastructure projects designed to facilitate global trade [10]. Furthermore, the emergence of bio-connected devices integrating biosensors, artificial intelligence, and blockchain is reshaping supply chain security, particularly for pharmaceutical and perishable goods. Despite high costs and significant implementation requirements, these technologies offer essential tools for ensuring traceability and operational reliability in the context of growing geoeconomic tension [11].

## 3. Internal Fault Lines in European Logistics

Beyond external pressures, European ports face significant structural fragmentation that undermines their operational coherence and strategic potential. Each EU member States manages its port infrastructure according to national priorities, without an overarching framework for coordination at the continental level. This results in inconsistent operational standards, often non-interoperable information systems, and, at times, counterproductive competition between proximate ports. The lack of harmonization slows technological innovation, complicates the adoption of resilient and sustainable logistical solutions, and impedes the creation of a unified EU maritime strategy. Resource dispersion and uneven flow management generate structural inefficiencies that compromise the continuity of trade within global supply chains, exposing Europe to considerable economic and geopolitical shocks. The absence of politically integrated governance weakens the EU's ability to resist external influence, including that of major foreign powers, and limits its capacity to exploit its full commercial potential. Any localized disruption in a single port can rapidly cascade across the continent, illustrating that genuine logistical sovereignty is unattainable without coordinated institutional reform and the integration of standardized digital and operational protocols.

While digitalization enhances efficiency and operational transparency, it also significantly increases vulnerability to cyber threats. According to the EU Agency for Cybersecurity, European port systems are frequently targeted by intrusions that disrupt terminal planning, container tracking, and logistical coordination [12]. In 2021, the Port of Antwerp, one of Europe's largest hubs, experienced a major cyberattack that temporarily halted operations, affecting several hundred containers and causing delays across approximately one hundred supply chains. Critical software systems and infrastructure are increasingly interconnected internationally, rendering Europe vulnerable to cyberattacks originating from any location, including through third-party suppliers or imported equipment.

Technium Social Sciences Journal
Vol. 79, 204-212, January, 2026
ISSN: 2668-7798
www.techniumscience.com

Addressing these risks requires substantial investments in cybersecurity, coupled with shared governance, harmonized protocols, and the development of a unified security culture among EU member States. By the end of 2025, these conditions remained insufficiently implemented, leaving ports exposed. Without such measures, the ongoing digital modernization risks amplifying vulnerabilities rather than mitigating them, transforming interconnectedness into a potential vector for systemic disruption.

Technological disparities among European ports exacerbate structural weaknesses and directly impact operational resilience. Rotterdam and Hamburg exemplify advanced smart port technologies, including automated terminals, digital twins, and AI-driven planning systems, which simultaneously enhance efficiency and security. In contrast, many Mediterranean and Eastern European ports remain largely analog, with minimal automation and predominantly human-centered management [13]. Limited investment, fragmented regulatory frameworks, and the absence of a cohesive EU strategic vision hinder the deployment of technology across the continent. This uneven modernization not only generates economic inefficiencies but also directly threatens logistical sovereignty, as less advanced ports are particularly susceptible to traffic disruptions, operational errors, and cascading failures. The interplay of heterogeneous infrastructures, fragmented information systems, and varying technical standards weakens the overall resilience of supply chains, constraining the EU's ability to respond rapidly and cohesively to external shocks or crises. Achieving a uniformly secure and efficient network demands substantial investment, regulatory alignment, and strategic coordination.

Political and economic rivalries between EU member States further compound structural vulnerabilities in port operations. National strategies often prioritize attracting traffic and investment to specific ports to stimulate domestic economic growth, frequently at the expense of regional cooperation and the collective optimization of EU maritime hubs [14]. Favorable tax regimes and incentives for certain ports may exacerbate these tensions, preventing the implementation of a unified policy for the security and modernization of infrastructure. This fragmentation limits the EU's capacity to establish standardized protocols for security, automation, and logistics planning. Recent incidents, including temporary Suez Canal blockages and severe delays at Rotterdam due to strikes or cyberattacks, illustrate how local disruptions can escalate into continent-wide challenges. The diagnosis is clear: Europe cannot claim credible logistical sovereignty until institutional fragmentation, technological disparities, and intra-EU rivalries are systematically addressed, enabling coordinated governance, technological convergence, and a resilient, continent-wide port system capable of withstanding future shocks.

## 4. Restoring Power to EU's Maritime Gates

Europe is currently at a pivotal point, confronting simultaneous and recurring disruptions that challenge the continuity of trade and the stability of its critical infrastructure. Strategic competition between China and the United States is reshaping maritime trade routes, investment patterns, and the management of essential ports, while the war in Ukraine and tensions in the Red Sea emphasize the fragility of EU supply chains. Added to these pressures is a rapid escalation in climate-related disasters, which no longer impact only localized regions but produce cascading effects across global commerce and national security. Hurricanes Beryl, Helene, and Milton in 2024, along with massive fires in New England, illustrate how localized events disrupt complex production and distribution networks.

Technium Social Sciences Journal
Vol. 79, 204-212, January, 2026
ISSN: 2668-7798
www.techniumscience.com

Similarly, in the United States, reduced water levels in the Mississippi River and the Panama Canal in 2022 paralyzed agricultural trade, demonstrating how regional hazards can generate worldwide repercussions [15]. In a polarized information environment, some foreign actors exploit these crises to disseminate disinformation, as exemplified during the Hawaii wildfires in 2023. For Europe, these dynamics reinforce the urgency of developing comprehensive strategies to secure ports as critical nodes, ensuring that logistical sovereignty remains actionable and enforceable.

*4.1. Explicit Inclusion of Logistics as a Strategic Component*

Integrating logistics into EU industrial strategy is essential to safeguard supply chain continuity and maintain economic sovereignty. Despite substantial EU investments in semiconductors and batteries for electric and hydrogen vehicles, these initiatives risk falling short if the physical flow of materials and components remains vulnerable. Mapping EU value chains, identifying critical vulnerabilities, and coordinating public and private investments in the most strategic ports are therefore indispensable. The Rotterdam-Ghent-Antwerp maritime corridor handles over one-third of Europe's container traffic and serves as a crucial conduit for essential electronic and chemical components [16]. A coordinated approach optimizes flow allocation between major hubs and secondary ports, mitigates congestion, and allows operational alternatives in case of geopolitical, climate, or health crises. Targeted EU financial instruments, including port-specific investment funds, can support infrastructure modernization and strengthen resilience. By treating logistics as a core strategic element, Europe can ensure that supply chains are not only technically efficient but also capable of sustaining autonomy, continuity, and adaptability in the face of multifaceted disruptions.

*4.2. Technological Modernization through Digitization and Automation*

Digitization and automation are critical to enhancing operational efficiency, resilience, and security across European ports. Rotterdam and Hamburg already leverage automated terminals, digital twins, and AI-driven containers planning to minimize delays and human errors while increasing throughput. Extending these technologies across the continent would establish an interoperable network capable of absorbing local disruptions and streamlining continental flows. IoT sensors, real-time tracking, and predictive analytics can reduce terminal waiting times by 15–20%, accelerating the import of critical goods such as electronic components and foodstuffs [17]. Standardized protocols and system interoperability enhance coordination between primary hubs and secondary ports, ensuring the continuity of flows during congestion or other disruptions. Beyond economic efficiency, digital infrastructure strengthens resilience against cyberattacks, strikes, or extreme weather events. By creating a unified technological ecosystem, the EU can transform its ports into a strategically coordinated network that anticipates, absorbs, and responds to external shocks [18], thereby ensuring that EU maritime logistics remain both secure and reliable.

*4.3. Cybersecurity and Strategic Protection*

As European ports become increasingly digitized and interconnected, they remain highly susceptible to cyberattacks and ransomware, necessitating a robust cybersecurity and strategic protection framework. Establishing a common European port cybersecurity framework, including technical standards, advanced intrusion detection systems, and redundant critical infrastructure, is indispensable [19]. Civil-military cooperation enables

Technium Social Sciences Journal
Vol. 79, 204-212, January, 2026
ISSN: 2668-7798
www.techniumscience.com

better crisis simulations, infrastructure security, and rapid response coordination during major threats. Joint exercises with port operators and armed forces help anticipate disruptions in the transport of critical materials, such as electronic components or lithium, thereby maintaining the continuity of supply chains. Effective EU-level coordination reduces dependency on foreign operators and limits the risks associated with data manipulation or sabotage. Integrating cybersecurity and civil-military collaboration strengthens confidence among economic actors in the stability and resilience of supply chains, ensuring that disruptions can be managed without threatening Europe's logistical and economic sovereignty [20]. These measures also provide the foundation for a long-term, proactive approach to safeguarding critical maritime infrastructure.

### *4.4. EU Cooperation and Common Standards*

EU member States must urgently harmonize security standards, share best practices and technologies, and coordinate political positions to limit foreign influence on critical maritime infrastructure. The creation of an EU Observatory for Port Logistics would centralize information on traffic flows, monitor risk levels, and anticipate external disruptions while supporting uniform deployment of smart technologies and cybersecurity measures. This coordinated approach transforms each port into an integral link of a resilient European network, capable of sustaining operations during crises. Financial and regulatory incentives for less modernized ports would facilitate technological and operational convergence, ensuring that all ports contribute effectively to continental resilience. Ultimately, the combination of common regulation, active cooperation, and strategic coordination strengthens Europe's autonomy, enhances supply chain resilience, and consolidates logistical sovereignty in the face of geopolitical, climatic, and health-related disruptions [21]. Through these initiatives, European ports can function as secure, adaptable, and strategically integrated nodes that support continental economic stability.

## 5. Conclusion

European ports now operate in an extremely unstable international environment, characterized by a proliferation of simultaneous and recurring crises. The strategic rivalry between China and the United States is reshaping global supply chains, while Russia remains at the center of a tense geopolitical dynamic, intensified by the ongoing war in Ukraine. In this context, the U.S. National Security Strategy (NSS), a formal strategic policy document outlining the administration's national security priorities and submitted to Congress at the start of a presidential term, expressed unusual concern about Europe's future in November 2025 [22]. According to the NSS, Europe faces structural economic decline and a weakening of political autonomy, consequences linked to internal EU dynamics, migration policies, and demographic challenges such as declining birth rates. The report emphasizes that, without corrective measures, some EU member States could become unreliable partners for the United States. In this framework, port infrastructure emerges as a critical test: control over these facilities determines Europe's ability to withstand external pressures and preserve strategic autonomy, highlighting that logistical sovereignty is a cornerstone of continental resilience and economic security.

The NSS further underscores a paradox with significant implications for Europe's logistical sovereignty: the war in Ukraine has increased the continent's dependence on external suppliers, particularly affecting Germany, whose industrial sectors have sought

*Technium Social Sciences Journal*
*Vol. 79, 204-212, January, 2026*
*ISSN: 2668-7798*
*www.techniumscience.com*

alternative sources, including China, to compensate for reduced Russian gas access. Major industrial projects, such as the construction of chemical plants in China relying on Russian energy, exacerbate Europe's structural vulnerabilities and diminish strategic autonomy. Yet, the document also reiterates that Europe remains indispensable to the United States for both global stability and transatlantic economic vitality. The U.S. strategy thus focuses on encouraging the strengthening of national sovereignty, enhancing defense responsibilities, and promoting economic policies capable of countering aggressive foreign practices, including technological espionage and cyber destabilization. Within this context, port sovereignty is identified as a key strategic dimension: modernizing port infrastructure and asserting operational autonomy are essential if Europe is to maintain its economic and political influence globally. Failing to address these challenges may leave Europe exposed to escalating external pressures and diminish its ability to act as a cohesive geopolitical actor.

**References**

[1] https://www.gat.report/73548/western-ligurian-sea-port-authority-hit-by-cyberattack/, Accessed September 10, 2025.
[2] https://fr.euronews.com/2022/02/03/en-europe-des-terminaux-petroliers-touches-par-une-vaste-cyberattaque, Accessed April 16, 2025.
[3] Berger, A., Khan, H., Schrank, A., & Fuchs, E. (2023). A new policy toolbox for semiconductor supply chains. *Issues in Science & Technology*, *39*(4), 39–42. https://doi.org/10.58875/TERK6342
[4] https://www.container-z.com/fr/blog/l-histoire-du-port-de-rotterdam, Accessed July 6, 2025.
[5] European Conference of Ministers of Transport (1993). *Short sea shipping: Round table 89*. Paris: Organisation for Economic Co-operation & Development.
[6] Bezat, J.-M. (2025). Comment la Chine tisse un réseau portuaire mondial. *Le Monde*, April 10. https://www.lemonde.fr/economie/article/2025/02/15/la-chine-tisse-un-reseau-portuaire-mondial_6547389_3234.html
[7] Grošelj, K. (2023). *Report on the security and defence implications of China's influence on critical infrastructure in the European Union*. Brussels: European Parliament.
[8] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/wdn-20250825-1, Accessed November 2, 2025
[9] Rohman, H., Sumarna, S., Suwanda, S., & Leksmanawati, W. (2022). Collaboration of ministries/institutions and the private sector in handling cyber threats through the establishment of *Computer Security Incident Response Team* (CSIRT). *Technium Social Sciences Journal*, *38*, 87–102. https://doi.org/10.47577/tssj.v38i1.7906
[10] Oprescu, G. (2020). Some measures to optimize and make efficient the international maritime transport. *Technium Social Sciences Journal*, *10*, 649–651. https://doi.org/10.47577/tssj.v10i1.1442
[11] Paché, G. (2024). Monitor to protect: The proliferation of bio-connected devices in supply chains. *Technium Social Sciences Journal*, *66*, 441–451. https://doi.org/10.47577/tssj.v66i1.12157
[12] De Sousa Figueiredo, R., Drougkas, A., Lella, I., Malatras, A., Naydenov, R., Stanic, Z., Theocharidou, M., & Tsekmezoglou, E. (2023). *ENISA threat landscape: Transport sector (January 2021 to October 2022)—March 2023*. Heraklion: EU Agency for Cybersecurity.

*Technium Social Sciences Journal*
*Vol. 79, 204-212, January, 2026*
*ISSN: 2668-7798*
*www.techniumscience.com*

[13] Brunila, O.-P., Kunnaala-Hyrkki, V., & Inkinen, T. (2021). Hindrances in port digitalization? Identifying problems in adoption and implementation. *European Transport Research Review*, *13*, Article 62. https://doi.org/10.1186/s12544-021-00523-0

[14] Luo, M., Chen, F., & Zhang, J. (2022). Relationships among port competition, cooperation and competitiveness: A literature review. *Transport Policy*, *118*, 1–9. https://doi.org/10.1016/j.tranpol.2022.01.014

[15] Picchione, K., & Finegan, L. (2025). The case for a national disaster research strategy. *Issues in Science & Technology*, *41*(4), 93–95. https://doi.org/10.58875/NTQF8421

[16] Kerbiriou, R., & Serry, A. (2020). *Le trafic portuaire des ports européens*. Le Havre: UMR IDEES CNRS.

[17] Aslam, S., Navarro, A., Aristotelous, A., Garro Crevillen, E., Martınez-Romero, A., Martínez-Ceballos, A., Alessandro Cassera, A., Orphanides, K., Herodotou, H., & Michaelides, M. (2025). Machine learning-based predictive maintenance at smart ports using IoT sensor data. *Sensors*, *25*(13), Article 3923. https://doi.org/10.3390/s25133923

[18] Tsoulfas, G. (2026). Port resilience: A systematic literature review. *Maritime Economics & Logistics,* forthcoming. https://doi.org/10.1057/s41278-025-00326-3

[19] Fredouet, C.-H., & Haouari, M. (2025). Cyber risk awareness and management: How mature are French ports regarding cybersecurity? *European Journal of Maritime Research*, *4*(1), 1–4. https://doi.org/10.24018/maritime.2025.4.1.30

[20] Valero, C. (2023). *La cybersécurité, un défi majeur pour le monde maritime*. Note de Synthèse No. 254. Saint-Nazaire: ISEMAR.

[21] https://smartmaritimenetwork.com/2025/07/18/nato-warns-of-growing-cyber-threat-to-port-infrastructure/, Accessed October 10, 2025

[22] https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf, Accessed December 3, 2025.