Cybersecurity, knowledge management and sustainability disclosure in DT-Enabled European ports

Assunta Di Vaio, Elisa Van Engelenhoven, Anum Zaffar and Gabriella D'Amore

Assunta Di Vaio is based at the Department of Law, University of Naples "Parthenope", Naples, Italy. Elisa Van Engelenhoven and Anum Zaffar are both based at the Department of Law, Blue Shipping & Cruise Laboratory (BSCLab), University of Naples "Parthenope", Naples, Italy. Gabriella D'Amore is based at the Department of Law, University of Naples "Parthenope", Naples, Italy.

Received 4 December 2025
Revised 9 March 2026
19 May 2026
Accepted 23 June 2026

Conflict of interest: The authors declare no conflicts of interest.

Abstract

Purpose – *This study aims to investigate how European ports disclose cybersecurity governance and knowledge management (KM) practices within digital twin (DT) technology environments as part of broader operational resilience and net-zero greenhouse gas emissions reduction.*

Design/methodology/approach – *This study uses qualitative content analysis of publicly available non-financial disclosures to investigate two leading European ports, i.e. Rotterdam and Hamburg, that have fully implemented the DT adoption process. Based on 36 documents (sustainability reports, DT roadmaps and innovation strategies) published between 2020 and 2024, the analysis focuses on cybersecurity and KM practices disclosed to stakeholders. By combining automated thematic extraction through Leximancer (Version 5) with manual interpretive coding, the study offers novel insights into how ports publicly frame and disclose DT-related cybersecurity and KM practices, contributing to both theory and practice in maritime digitalization.*

Findings – *Results reveal significant heterogeneity in the scope and depth of cybersecurity and KM disclosures among ports operating within DT frameworks. One port predominantly frames cybersecurity as an operational safeguard, while the other discloses cybersecurity within broader KM-oriented governance practices associated with data-driven decision-making and net-zero emission targets.*

Originality/value – *This study responds to limited research examining the intersection of cybersecurity, KM and DT in port digitalization, particularly through the lens of stakeholder-oriented disclosure. By adopting a comparative case study approach focused on official reporting, it offers novel insights into how ports construct legitimacy and accountability around secure knowledge flows publicly linked to environmental objectives. The results contribute to theory by bridging cybersecurity governance, KM and sustainability disclosure within DT-enabled infrastructures.*

Keywords *Digital twins, Cybersecurity governance, Knowledge management, Sustainability disclosure, Stakeholder legitimacy, Port decarbonization*

Paper type *Research paper*

1. Introduction

The adoption of digital twin (DT) technology is reshaping European port operations by enabling advanced, data-driven planning, monitoring and optimization that can improve both operational efficiency and environmental performance (Tao *et al.*, 2019). In this context, DTs act as critical enablers for designing, tracking and refining decarbonization strategies, aimed at reducing greenhouse gas (GHG) emissions. Yet accelerated digitalization also widens the attack surface and increases dependencies on data integrity, availability and confidentiality, making cybersecurity and knowledge management (KM) pivotal capabilities. Sensitive operational and environmental data must circulate securely and reliably across complex multi-actor ecosystems including port authorities, terminal operators, shipping companies, regulators and technology providers (ENISA, 2022; Heilig and Voß, 2017). Despite extensive research on the environmental and operational advantages of DTs, the

convergence of digital transformation, cybersecurity, KM and decarbonization remains insufficiently theorized and empirically examined (Alamoush *et al.*, 2022; Di Vaio *et al.*, 2025a, 2025b, 2025c).

Moreover, the COVID-19 pandemic accelerated digital transformation in port ecosystems by increasing reliance on remote operations, automated coordination and real-time data exchange. As dependence on DT-enabled infrastructures grew, ports became more exposed to cyber threats, while cyber incidents and governance responses increasingly generated organizational learning signals that could be captured, codified, shared and reused through KM processes. From this point of view, cybersecurity-related reporting is not seen only as a compliance-driven reporting process, but as a way for organizations to share the knowledge acquired in their operations, learn about cybersecurity risks and articulate governance frameworks and learning processes to internal and external audiences. Hence, this study focuses on the disclosure of cybersecurity governance and cybersecurity-related KM practices in DT-enabled port environments. Accordingly, KM is adopted as the focal analytical lens through which cybersecurity governance is examined in DT-enabled port environments.

Although research on cybersecurity governance and digital transformation is expanding, there has been limited focus on the management and disclosure of cybersecurity-related knowledge within digitally enabled port ecosystems. The current literature frequently addresses cybersecurity from primarily technical or operational viewpoints, leaving the KM aspects of cybersecurity governance and disclosure largely unexplored, especially in the port sector after the rapid digitalization prompted by the COVID-19 pandemic. Prior research has addressed individual components, including DT adoption (Cunha *et al.*, 2025), cybersecurity in port logistics (Heilig and Voß, 2017), KM linked to digital strategies (Wang and Li, 2023) and GHG accounting in DT contexts (Di Vaio *et al.*, 2025a, 2025b, 2025c), but rarely integrates these dimensions within analyses of official port disclosures. In addition, previous studies have not sufficiently integrated KM processes with stakeholder-focused disclosure practices in digitally interconnected operational environments (Bebbington *et al.*, 2008; Di Vaio *et al.*, 2024).

Hence, to address this gap, the research question (RQ) of this study is:

RQ1. How do ports manage knowledge derived from cybersecurity practices within digital twin environments to build legitimacy with stakeholders, enhance operational resilience, and support greenhouse gas emissions reduction?

Cybersecurity activates learning signals in the form of detected vulnerabilities, near misses and control failures. The codification of these signals is carried out with the help of KM artefacts, including playbooks, revised procedures, training modules and after-action reviews. In turn, these knowledge processes can improve operational resilience and support emissions-relevant decision-making.

Therefore, answering our research question, we analyze public disclosures (sustainability reports and strategic documents) as a lens on the strategic narrative ports construct to demonstrate accountability and compliance with evolving sustainability mandates (Higgins *et al.*, 2018; Neugebauer *et al.*, 2024).

Our study suggests 2 × 2 typology (cybersecurity governance depth × KM maturity) as an explanatory approach, not as a descriptive one. Different configurations illuminate when cybersecurity is largely technical and compliance-based and when it is turned into institutionalized knowledge governance, enabling organizations to communicate DT-enabled emissions decisions and enforce stakeholder-based disclosure practices.

Methodologically, we conduct a comparative qualitative content analysis of documents published between 2020 and 2024, a period of intensified digitalization and sustainability initiatives in European ports. At this stage, ports have expedited digitalization and remote

operational capacities to ensure continuity in the face of mobility restrictions and supply-chain disruption. Meanwhile, extended digital interfaces and decentralization of workflows enlarged the cyber-attack area, exposing the system and its vulnerabilities to phishing, ransomware, and other attacks. These changes enhanced resilience, transparency and safe data governance. Two cases, Rotterdam and Hamburg, are purposively selected following Neugebauer *et al.* (2024) based on their DT maturity. We combine automated thematic mapping using Leximancer (Smith and Humphreys, 2006) with manual interpretive coding, coupling computational breadth with contextual depth to identify dominant themes and to interpret how cybersecurity and KM are framed and disclosed as enablers of digital governance and the net-zero transition.

The principal contribution of this study is its conceptualization of cybersecurity governance as a valuable form of organizational knowledge that can be reused within digital transformation-enabled port ecosystems. By framing cybersecurity events and governance procedures as signals for organizational learning, the study elucidates the processes by which such knowledge can be codified, disseminated and disclosed through KM mechanisms in digitally interconnected operational settings.

2. Literature review

This study is primarily grounded in a KM perspective on how ports in DT-enabled environments manage cyber security information and organizational learning processes. KM theory focuses on the development, codification, sharing and reusing of organizational knowledge to enhance decision-making, operational coordination and adaptability. In highly digitalized port ecosystems, cybersecurity events and governance activities create valuable knowledge about vulnerabilities, operational risks, incident response and system reliability. Therefore, cybersecurity governance in a DT environment requires organizational mechanisms to turn cyber-related information into reusable knowledge resources.

In addition, the study selectively relies on stakeholder and legitimacy arguments to back this central KM position. The stakeholder-driven governance approach implies that the disclosure of cybersecurity information is important for organizations to minimize information asymmetry and to show accountability to regulators, investors, supply chain partners and other stakeholders. However, these perspectives do not provide an independent theoretical basis but are used as explanatory mechanisms. Similarly, resilience is not treated as an independent theoretical framework, but as an operational implication of cybersecurity-related KM practices in digitally connected port systems.

2.1 Linking cybersecurity and knowledge management in digital twin-enabled port ecosystems for sustainability advancement

We define the intersection of cybersecurity and KM in DT-enabled port ecosystems. Maritime digitalization is accelerating and, with it, the complexity and interconnection of port information systems also (Schinas and Metzger, 2023). In such contexts, cybersecurity must be conceived not only as a suite of technical controls, such as encryption, multi-factor authentication, systematic patching and hardening, but also as an organizational capability governed through policies, risk assessment, training and compliance with regulatory frameworks including network and information systems directive 2 and general data protection regulation (Cheung *et al.*, 2021; Mehmood *et al.*, 2019; Nankya *et al.*, 2023; Ometov *et al.*, 2018; Progoulakis *et al.*, 2023; Senarak, 2024; Tam *et al.*, 2021). When this sociotechnical alignment is weak, operational inefficiencies emerge and may translate into longer waiting times, additional rework and ultimately higher emissions, thus diluting the environmental promise of digitalization (de la Peña Zarzuelo, 2021).

In this study, we define KM as the systematic ability by which organizations generate, codify, share and institutionalize as well as reuse knowledge to facilitate coordinated action

and adjustment (Nonaka and Takeuchi, 1995; O'Dell and Grayson, 1998). Whereas other similar views like the organizational learning and dynamic capabilities accentuate adaptation in the face of uncertainty, KM anticipates the artefacts, routines, repositories and governance organizations that make knowledge enduring and transferable across the organizational boundaries. This structured knowledge ability in DT-enabled ports defines whether cybersecurity knowledge will still be episodic reactions or be institutionalized as an operational and environmental performance driver. In practice, this involves documenting incident response playbooks and threat models, maintaining lessons-learned repositories and security bulletins, institutionalizing after-action reviews and cross-functional exercises and monitoring coverage and reuse through simple metrics such as time-to-codify, adoption rates of updated procedures, near-miss capture and the speed with which knowledge propagates across units (O'Dell and Grayson, 1998; Wang and Wang, 2019).

This study builds upon the KM perspective and considers cybersecurity governance as a source of reusable organizational knowledge. In the digitally connected port ecosystems, such knowledge can be incorporated in organizational routines, port governance practices, training programs and disclosure processes to enable operational coordination and communication with stakeholders. While the adoption of DT, cybersecurity governance and KM practices have been studied separately, the combination of these within stakeholder-oriented disclosure processes has not been investigated.

Theoretical perspectives converge on the same implication. Stakeholder theory explains how environmental and social imperatives are translated into firm-wide action and legitimacy (Calderaro and Craig, 2020; Papa *et al.*, 2021; Sahoo, 2024). Socio-technical systems [ship-to-ship (STS)] theory emphasizes the inseparability of human, organizational and technological elements in secure digital infrastructures (Bostrom and Heinen, 1977; Troyer, 2017). The knowledge-based view (KBV) treats knowledge embedded in people, routines and infrastructure as a strategic asset for adaptation under uncertainty (Alvarenga *et al.*, 2020). In DT-enabled ports, cybersecurity delivers sustainability value when it is embedded in institutionalized KM that reliably carries learning into operational decisions.

Cyber incidents generate operational knowledge about vulnerabilities, responses and system dependencies. The value of this knowledge depends on both technical protections and the organization's ability to codify, share and reuse it. Organizations that document and distribute cyber events and insights are better able to refine their procedures, reducing delays, fuel use and emissions. Table A1. (see Appendix) Outlines the main constructs and their implementation in DT-Enabled ports.

2.2 Cybersecurity and knowledge management in the context of digital twin adoption for sustainable port operations

Operational resilience is increasingly important in digitalized port ecosystems where operations rely on interdependent digital infrastructures and ongoing data exchange (Salvi *et al.*, 2022). In this context, resilience is defined as the capacity of organizations to predict, to absorb and recuperate interruptions and to continue functioning. In DT surroundings, this ability is strictly connected with cybersecurity governance and KM. Cyber incidents, vulnerabilities and threat-intelligence signals create learning opportunities which when recorded and shared in the KM mechanisms such as training, procedures and knowledge sharing have the potential of enhancing organizational preparedness and adaptive capacity (Faleiro *et al.*, 2021).

In DT-enabled ports, sustainability gains depend on much more than simulation and predictive analytics. They require secure data governance and a KM capability that can keep pace with dynamic, high-volume information flows. Moving beyond reactive mitigation, many organizations adopt proactive methods such as threat modeling, which systematically identifies and analyzes potential vulnerabilities in maritime cyber-physical systems and

informs anticipatory defenses that evolve as the threat landscape changes (Erbas *et al.*, 2024; Yu *et al.*, 2023). KM makes these approaches operational by integrating explicit knowledge, such as policies and incident logs, with tacit operator expertise, so that vulnerability identification, adaptive defense and sustainability goals are aligned rather than sequential (Uden and He, 2017). AI and machine learning augment KM by detecting complex patterns and issuing early warnings before cyber disruptions degrade operational or environmental performance (Leoni *et al.*, 2024).

Experiences related to cybersecurity gain value when embedded within routines, governance protocols, repositories, training initiatives and mechanisms for cross-functional knowledge sharing. This approach expands traditional discussions of cybersecurity beyond technical risk management by underscoring the organizational processes that enable the retention and reuse of cyber-related knowledge in digitally transformed environments.

Efficiency relates to turnaround times, throughput and resource utilization; reliability concerns the consistency and predictability of services; and safety and security compliance reflect adherence to applicable laws and best practices designed to protect people, assets and the environment (Chlomoudis *et al.*, 2024; World Bank, 2021, 2025; Yang *et al.*, 2014). Safety focuses on preventing accidental harm and benefits from indicators such as incident rates, near-miss reporting and compliance measures, while security focuses on intentional threats and depends on posture, audits and response readiness (Tseng and Pilcher, 2017; UNCTAD, 2022). KM links cyber learning to operational decisions that have emissions implications.

Despite conceptual clarity, an operational gap persists. There is still limited empirical evidence on how proactive cybersecurity approaches such as threat modelling are combined with KM in day-to-day practice in DT-enabled ports, and with measurable effects on resilience, stakeholder confidence and environmental performance. Table A2. represents the port performance dimensions where KM-cyber links to environmental outcomes (see Table A2 in the Appendix).

2.3 Integrating cybersecurity, knowledge management, and digital twin for stakeholder-oriented reporting

The International Maritime Organization has required that cyber-risk management be embedded within safety management systems (de la Peña Zarzuelo, 2021). In parallel, ports remain critical infrastructures with non-trivial environmental impacts, variously estimated to account for a meaningful share of global GHG emissions, so that digitalization and DT adoption in particular, act simultaneously as levers for operational resilience and environmental accountability (Di Vaio *et al.*, 2025a, 2025b, 2025c; Notteboom *et al.*, 2022).

Cybersecurity measures produce knowledge that is central to digital governance. Explicit elements include policies, incident logs, threat models, configuration baselines, audit trails and documented response procedures; tacit elements comprise operator expertise, anomaly recognition and contextual judgment under time pressure. Effective KM captures, protects, stores, disseminates and reuses this knowledge so that vulnerabilities are identified earlier, defenses can adapt and decision-making improves without compromising confidentiality (Alsehrawy *et al.*, 2022; Di Vaio *et al.*, 2025a, 2025b, 2025c; Uden and He, 2017).

This study uses stakeholder and legitimacy perspectives to elucidate the disclosure dimension of cybersecurity-related KM practices. Within digitally interconnected port ecosystems, organizations encounter heightened expectations from regulators, investors, logistics partners, and other stakeholders regarding transparency in cybersecurity governance and digital risk management.

From stakeholder and legitimacy standpoints, disclosure functions as a governance tool rather than a procedural requirement. In this research, credible disclosure is conceptualized as the reporting of tangible process evidence rather than declarative statements. In contrast, process evidence encompasses observable routines and artefacts such as named incident-response procedures, after-action reviews, formal training programs, knowledge repositories, reuse metrics or cross-functional governance boards.

Reports that describe concrete processes, naming the artifacts that store knowledge, the learning loops that spread it and the reuse or coverage measures that track it, help stakeholders evaluate whether ports are credibly translating cyber learning into operational and environmental outcomes (Bebbington *et al.*, 2008; Dowling and Pfeffer, 1975; Freeman, 1984; Higgins *et al.*, 2018; Suchman, 1995). However, a port-specific reporting architecture that integrates cybersecurity, KM, DT use cases and environmental indicators is still nascent, which limits comparability and assurance (de Vicente-Lama *et al.*, 2023; Homayouni *et al.*, 2025). The International Association of Ports and Harbors (IAPH) Cybersecurity Guidelines emphasize structured staff training and organizational awareness as foundations of governance, and these principles appear in public communications by ports such as Hamburg (IAPH, 2021; Port of Hamburg, 2021). Yet disclosures frequently under-specify the concrete training programs, the cadence and content of cyber drills and the measures used to monitor learning and reuse. The summary of how credible disclosure looks like and the common gaps noted in practices is represented in Table A3 (see Appendix).

By reading sustainability reports and strategic documents through the lenses of stakeholder and legitimacy theory, and by treating KM as the capability that institutionalizes cybersecurity learning, the analysis can identify when public disclosures provide sufficient process evidence to support credible claims about how digital resilience underpins environmental performance.

Figure 1 shows the theoretical framework of this study.

3. Methodology

3.1 Research design

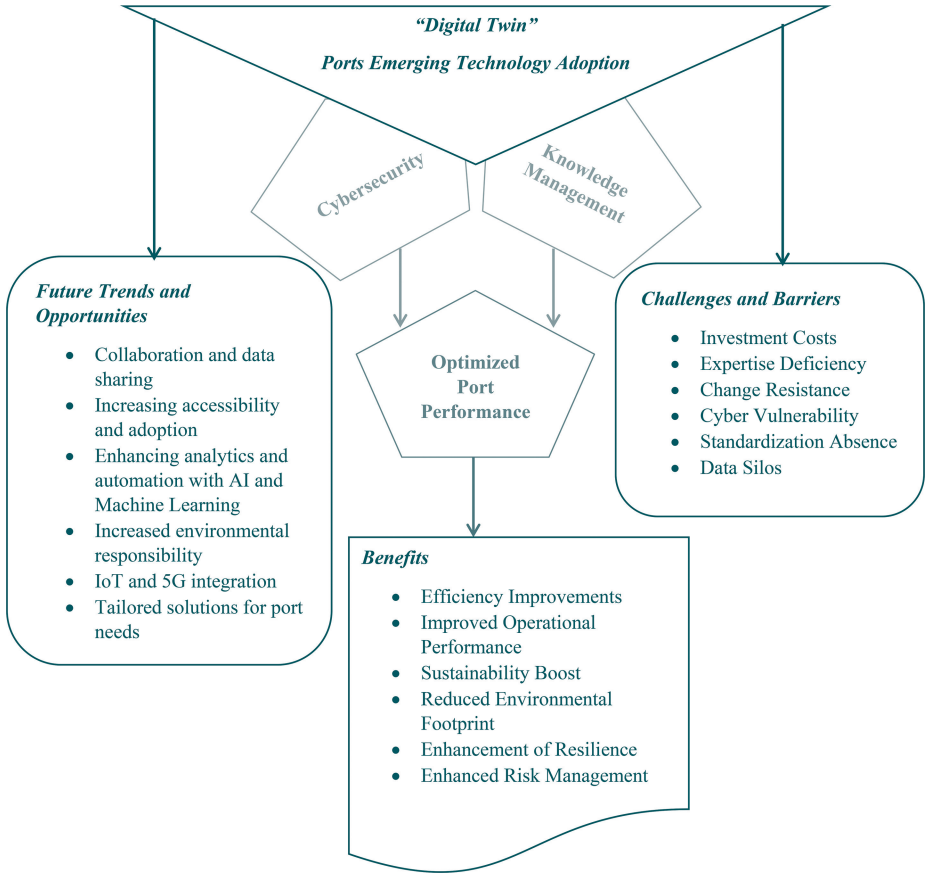
This study uses a qualitative content analysis to explore how European ports disclose cybersecurity and KM practices within fully implemented DT environments, addressing key research gaps related to the integrated management and communication of these domains in support of decarbonization and stakeholder engagement (Alamoush *et al.*, 2022; Cunha *et al.*, 2025; Di Vaio *et al.*, 2025a, 2025b, 2025c; Heilig and Voß, 2017; Neugebauer *et al.*, 2024; Wang and Li, 2023).

Content analysis is a well-established methodology for examining corporate disclosures, enabling the systematic identification of thematic patterns and textual relevance, particularly in sustainability reporting research (Guthrie *et al.*, 2004; Lozano and Huisingh, 2011; Steenkamp and Northcott, 2007; Torelli *et al.*, 2019; Unerman, 2000). Integrating both quantitative and qualitative approaches (Beck *et al.*, 2010), this study combines automated thematic extraction via Leximancer (Version 5) with manual interpretative coding to provide computational rigor alongside contextual depth.

3.2 Sampling strategy and data sources

Following Neugebauer *et al.*'s (2024) framework on DT maturity, two case studies, Rotterdam and Hamburg, were purposively selected as the only European ports with fully implemented and comprehensive DT systems. This choice facilitates an in-depth investigation of how cybersecurity and KM practices are operationalized and disclosed in advanced digital environments to enhance operational resilience, stakeholder legitimacy

Figure 1 Conceptual framework for digital twins adoption in European port strategies



Source: Authors' own compilation

and GHG emissions reduction. The selection of these two case studies is intended to enable analytical generalisation rather than statistical representativeness, allowing for the identification of recurring patterns across advanced digital port environments (Ghemawat and Khanna, 2003). Accordingly, the 2 × 2 typology was used as a heuristic framework to compare disclosure patterns across the two port cases in relation to cybersecurity governance depth and KM maturity.

The empirical data set comprises 36 documents, including sustainability reports, digital transformation roadmaps and innovation strategies published between 2020 and 2024. This period corresponds to a pivotal phase marked by accelerated digitalization in European ports, influenced by policy drivers such as the European Commission's Sustainable and Smart Mobility Strategy (European Commission, 2020), technological advancements and increasing environmental commitments.

Data collection involved a systematic review of official port websites to retrieve relevant disclosures between June and October 2025, encompassing DT adoption, cybersecurity, KM practices and environmental strategies. In fact, the study does not directly observe internal organisational practices, but it rather focuses on how ports publicly communicate and make visible cybersecurity, KM and DT-enabled governance. This choice is grounded in the relevance of public disclosures as analytical sources, as they reveal how ports construct accountability and legitimacy toward stakeholders by communicating strategic

priorities, responsibilities and governance commitments. Nevertheless, the integration of multiple secondary data sources, combined with the sequential use of automated and manual content analysis, enhances the credibility and depth of the findings (Di Vaio *et al.*, 2025a, 2025b, 2025c). Although these disclosures do not directly reveal internal practices, they remain analytically relevant as they reflect how organisations signal priorities, accountability and resilience to external stakeholders (Landrum and Ohsowski, 2018; Torelli *et al.*, 2019; Di Vaio *et al.*, 2025a, 2025b, 2025c). To maintain a focused analytical scope, decarbonization is treated as an outcome dimension rather than as an independent analytical pillar.

These documents represent rich knowledge artefacts that encapsulate organizational narratives, policy responses and innovation pathways (Table 1).

All documents were archived and catalogued to ensure traceability and replicability of the data set. Inclusion criteria comprised publicly available documents explicitly addressing digitalization, cybersecurity, KM practices or environmental strategies, while purely financial or non-relevant communications were excluded.

The content analysis was structured along three dimensions: cybersecurity, focusing on management of cyber risk, data security and resilience linked to digital infrastructures supporting GHG reduction (ENISA, 2022); KM, investigating collaborative knowledge flows, learning and decision-making in carbon reduction (Del Giudice *et al.*, 2017; Nonaka and Takeuchi, 1995); and GHG emissions, analysing DT applications for tracking and reducing emissions in port operations (Alamoush *et al.*, 2022; Di Vaio *et al.*, 2025a, 2025b, 2025c).

3.3 Coding framework development

To strengthen coding reliability, the four authors adopted a structured cross-check procedure. Author 1 and Author 2 independently coded the full data set using the theory-informed codebook developed from the literature and refined through the exploratory Leximancer outputs. Specifically, the codebook is structured around cybersecurity governance, KM routines and artefacts, DT-enabled operational knowledge flows and stakeholder legitimacy. To ensure consistency across heterogeneous disclosure formats, the codebook distinguished between explicit evidence, including references to training, procedures, cybersecurity initiatives and inter-organisational knowledge-sharing mechanisms, and implicit evidence, including references to data-driven coordination, real-time information exchange and digitally embedded learning processes. Author 3 and Author 4 subsequently reviewed and validated the coding outputs, focusing on the consistency of category attribution, the interpretation of ambiguous evidence and the alignment between the final categories and the theoretical framework. Cases of disagreement or uncertain classification were discussed collectively among the authors until consensus was reached. Through this iterative process, the codebook was progressively refined by clarifying category definitions, inclusion criteria and illustrative examples.

Table 1 Selected European ports' sustainability reporting and website pages

			Non-financial disclosure documents		
Port	*Mio.grosstons/year*	*Level of digital twin*	*Sustainability reporting*	*Website pages*	*Years*
Hamburg	111.8	Digital twin	3	10	2020–2024
Rotterdam	436.8	Digital twin	6	16	2020–2024

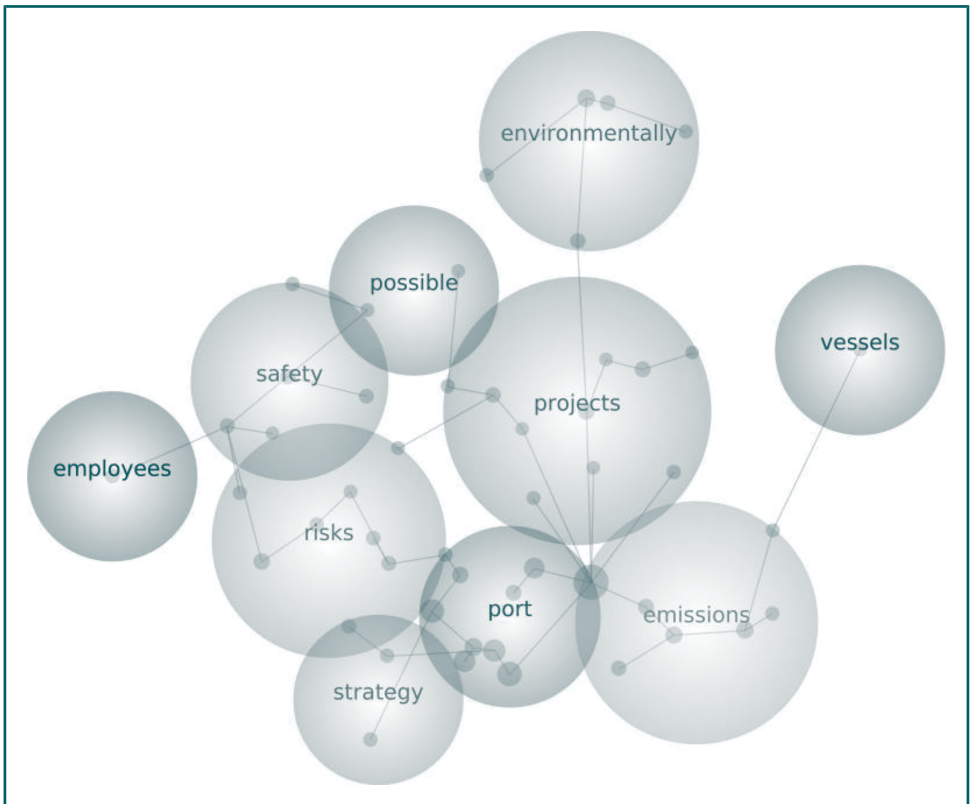
Source(s): Authors' data collection of the selected European Ports' Sustainability Reporting and Website Pages published between 2020 and 2024

3.4 Data analysis

The analysis followed a sequential integration workflow in which automated outputs informed theory-driven manual coding. Leximancer (version 5) facilitated automated thematic coding, identifying clusters of related concepts and visualizing key themes and their interrelationships (Crofts and Bisman, 2010; Smith and Humphreys, 2006). The software is used as an exploratory mapping tool to identify patterns of word co-occurrence and to map the semantic structure of the data set. The aim is to provide a preliminary overview of recurrent concepts and semantic associations, rather than as the main basis for theoretical interpretation. These outputs serve as a preliminary layer of analysis that supports, but does not replace, the interpretative coding process (Di Vaio *et al.*, 2025a, 2025b, 2025c). The authors implemented a systematic procedure before running the analysis, to extract meaningful concepts based on word association and proximity. First, the collected documents were grouped into individual folders corresponding to each selected European port, differentiating between sustainability reports and web content. Second, the files were uploaded into Leximancer (Version 5) and analysed using an unsupervised concept-seeding approach. Common function words and non-informative terms (e.g. "and," "used," "based") were manually removed from the concept seeds to refine the output. Moreover, singular and plural forms of semantically equivalent words (e.g. "port/ports," "employee/employees") were consolidated. Third, the software generated concept maps using default map generation settings, illustrating the main themes and their interrelationships within the analysed materials (Figure 2).

While Leximancer provides valuable support for automated text analysis, the core analytical contribution of the study derives from the manual comparative coding. Conducting a

Figure 2 Thematic map of the selected European Ports' non-financial disclosure documents published from 2020–2024



Source: Authors' own creation from Leximancer (V.5)

manual content analysis using a set of keywords commonly adopted in the literature is essential to deepen the interpretation of results and to clarify how port authorities disclose and manage critical digital infrastructure, with particular emphasis on data security and knowledge flows within the port ecosystem (Engstrom *et al.*, 2022). To enhance the reliability of this manual coding process, a double-coding approach was applied, whereby two independent coders examined the same data set and subsequently compared their outputs to resolve discrepancies. As evidenced in Table A4 in the Appendix, to enhance transparency and replicability, the authors operationalised the 2 × 2 typology (Cybersecurity Governance Depth and KM Maturity) through explicit scoring criteria. Cybersecurity governance depth was assessed based on the extent to which ports disclosed structured and coordinated practices, including monitoring systems, incident response mechanisms and inter-organisational initiatives (e.g. cyber resilience networks). KM maturity was evaluated by considering both explicit references and implicit evidence of knowledge processes, such as training activities, knowledge-sharing platforms and the integration of learning mechanisms within digital and operational workflows. Each dimension was coded on a binary scale (low/high) based on the presence of isolated versus systemic and embedded practices, ensuring consistency across cases despite heterogeneous disclosure formats. Each category was defined with inclusion criteria and illustrative examples to enhance coding consistency and replicability. The following keywords were selected based on an analysis of the existing literature: "digital," "digital-twin," "smart-ports," "cybersecurity," "security," "knowledge," "knowledge-management," "knowledge-sharing," "technologies," "decarbonization."

The analysed European ports do not rely on a uniform reporting framework. Instead, most relevant information, particularly concerning digitalization efforts, is disclosed through website pages, which tend to be more up-to-date and reflective of ongoing technological developments compared to formal sustainability reports. Hence, the manual content analysis was conducted on all the selected non-financial disclosures (NFDs), including reports, website pages and innovation strategies, to capture a more comprehensive and current picture of ports' digital and sustainability practices.

4. Results

4.1 Automated content analysis: Leximancer (ver. 5)

Figure 3 shows the "WordCloud" generated from the 50 most frequent words identified across the selected sustainability reports and website pages. The size of each term reflects its relative frequency within the selected documents. As illustrated, the most prominent

Figure 3 Word Cloud

Source: Authors' own creation from Word Cloud Generator

words are “smartport,” “digital,” and “authority,” providing an initial descriptive overview of the data set.

Leximancer was used to provide a preliminary overview of how key themes and concepts emerge within ports’ digital and environmental strategies.

The 36 analysed documents produced 10 themes and 50 concepts. The key themes that emerged from the analysis were: port, projects, emissions, risks, environmentally, safety, strategy, possible and employees (Table 2). These themes emerged as the most prevalent within the cluster, as indicated by their high frequency of occurrence and strong connectivity, reflecting their relative importance.

Port is the most relevant theme with the highest connectivity rate. It is related to concepts like “sustainable,” “management,” “climate,” “value,” “infrastructure,” “business,” “development,” and “supply.”

The theme “risks” is central to the analysis, and it is strongly linked with concepts like “impact,” “chain,” “future,” “security,” “digital,” “partners,” and “control.” On the other hand, the theme “safety” emerges as key dimension, associated with concepts like “measures,” “environment,” “information,” and “process” (Figure 4).

The concepts “environmentally,” “sustainable” and “emissions” emerge as highly relevant, suggesting the focus of the selected ports on decarbonization targets and goals (Table 3).

Also, the concept “digital,” which appears in the analysis with a relatively low likelihood, is linked to important concepts like “incidents,” “network,” “data,” “control,” “chain,” “supply,” “system,” “infrastructure,” “security,” and “traffic” (Figure 5).

The co-occurrence of “digital,” “security,” and “supply” suggests a strong association between digitalization and operational processes.

4.2 Manual content analysis

The manual content analysis shows that the selected European ports publicly frame digitalization and DTs as strategic infrastructures for improving efficiency and supporting the net-zero transition. When examined through a KM lens, the reports analysed describe how digitalization initiatives in both ports can implicitly generate and mobilize knowledge flows, indirectly support operational coordination and emissions-related decision-making. In particular, digital technologies are presented as enabling data-driven optimisation of port operations, including traffic management, berth allocation and energy efficiency strategies. The Port of Rotterdam describes the link between digital technologies and data-driven decision-making for emissions monitoring and reduction, and to stakeholder coordination in the energy transition, for instance through tools supporting port call optimisation and real-

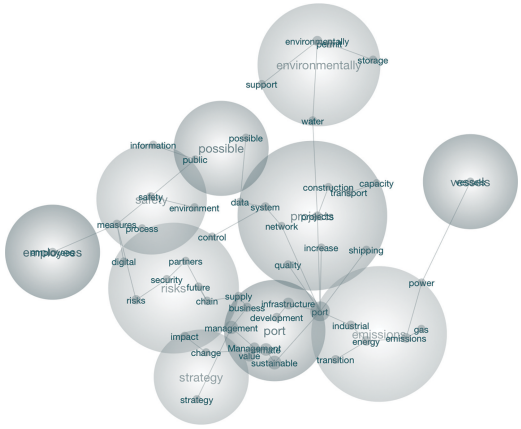
Table 2 Themes and related concepts in sustainability reporting and website pages

The selected European Ports with Concepts 100% and Theme size 35%

Theme	*Hits*	*Connectivity*	*Concepts*
Port	3037	19455.00	Port, sustainable, management, climate, value, infrastructure, business, development, supply
Projects	1463	5237.00	Projects, transport, system, shipping, data, quality, construction, increase, capacity, network
Emissions	1108	4624.00	Emissions, energy, industrial, transition, gas, power
Risks	1259	4555.00	Risks, impact, chain, future, security, digital, partners, control
Environmentally	1184	3531.00	Environmentally, permit, water, support, storage
Safety	967	2775.00	Safety, measures, environment, information, process
Strategy	347	1021.00	Strategy, change
Possible	292	760.00	Possible, public
Employees	268	565.00	Employees

Source(s): Authors’ processing of the European Ports’ Sustainability Reporting and Website Pages (2020–2024) using Leximancer (V.5)

Figure 4 Concept map of the selected European Ports' non-financial disclosure documents published from 2020–2024



Source: Authors' own creation from Leximancer (V.5)

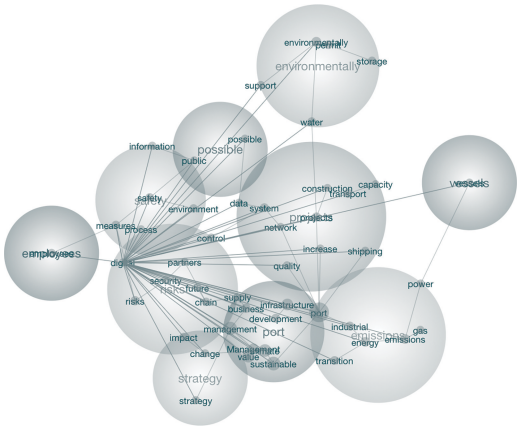
Table 3 Most frequent concepts

Concept	*Count*	*Likelihood (%)*
The selected European Ports with Concepts 100% and Theme size 35%		
Port	1,695	100
Environmentally	751	44
Sustainable	472	28
Harmful	396	23
Emissions	372	22
Management	326	19
Energy	306	18
Risks	299	18
Storage	291	17
Infrastructure	288	17
Projects	287	17
Safety	231	14
Transport	212	13
Water	209	12
Climate	201	12
Information	192	11
Transition	189	11
System	187	11
Impact	186	11
Measures	182	11
Strategy	171	10
Digital	161	9
Shipping	159	9
Security	157	9

Source(s): Authors' processing of the European Ports' Sustainability Reporting and Website Pages (2020–2024) using Leximancer (V.5)

time traffic management (Port of Rotterdam, 2024a, 2024b). From a KM perspective, the description of these practices suggests an ongoing process of knowledge production and circulation across organisational boundaries (Port of Rotterdam, 2024a, 2024b). Similarly, the Port of Hamburg presents digital solutions such as real-time traffic optimization systems and digital infrastructure projects aimed at improving efficiency and reducing emissions

Figure 5 Concept map of the selected European Ports' non-financial disclosure documents published from 2020–2024 displaying the relation of the concept "digital" with other concepts



Source: Authors' own creation from Leximancer (V.5)

(Port of Hamburg, 2025). While the discourse emphasizes integration, collaboration and continuous refinement, the reference to KM practices remains implicit and is not translated into clearly identifiable organizational learning structures.

Digitalization is thus presented primarily as an infrastructural enabler rather than as a formal knowledge governance system. The analysed documents further emphasize stakeholder collaboration as a prerequisite for implementing digitalization strategies. At the KM level, this emerges through references to knowledge sharing for logistics coordination, energy transition and real-time information exchange, particularly in the case of Rotterdam. Standardized data sharing is associated with greater ecosystem resilience and collective situational awareness. However, the disclosures do not specify formal KM architectures such as shared repositories, structured learning protocols or inter-organizational knowledge governance arrangements, suggesting that knowledge flows remain largely informal or technologically embedded.

The selected documents also describe the development and adoption of DT. Rotterdam's DT, which integrates container terminal processes and container flows and is being expanded toward autonomous navigation, functions as a platform for combining infrastructural, environmental and logistical knowledge (Neugebauer *et al.*, 2024; Port of Rotterdam, 2025b). From a KM perspective, the disclosures do not clarify how DT – which can be used as knowledge integration device – validates, storages, updates or systematically reuses knowledge over time. Similarly, Hamburg's BIM-based DT is described as a repository tool where "all relevant data and information are recorded, managed, and exchanged" among project participants. This directly supports the interpretation of the DT as a knowledge integration device, while still avoiding claims about full KM implementation (Port of Hamburg, 2025).

Regarding cybersecurity, the analysed documents highlight increasing strategic attention to digital risks and resilience. The Port of Rotterdam frames digital resilience as a core element of its broader strategy for flexibility, supply-chain continuity and strategic autonomy (Port of Rotterdam, 2025a, 2025b). In this area, KM-related evidence is more explicit than in other dimensions. Rotterdam's participation in the FERM Foundation's Cyber Strategy for Dutch Seaports can be interpreted as disclosure-based evidence of inter-organisational

knowledge sharing, particularly in relation to threat intelligence, awareness raising and collective cyber resilience (FERM, 2025). Similarly, internal instruments such as codes of conduct addressing phishing and digital risks suggest mechanisms of cybersecurity knowledge codification and dissemination at the employee level (Port of Rotterdam, 2024b). Moreover, Rotterdam describes the secure chain as a collaboration between industry and government aimed at "making port logistics more digitally resilient" (Port of Rotterdam, 2024b). At the sectoral level, the IAPH Cybersecurity Guidelines, promoted also by the Port of Hamburg, describes training and organizational awareness as foundational KM practices for cybersecurity governance (IAPH, 2021; Port of Hamburg, 2021). Nevertheless, despite these strategic references, the analysis reveals a limited disclosure on the operationalization of KM. Information regarding the structure and frequency of cybersecurity training, the presence of formal learning cycles or after-action reviews, the mechanisms for capturing and reusing incident-based knowledge and the use of KM metrics to assess learning effectiveness is largely absent.

The cross-case comparison highlights both convergence and heterogeneity in the analysed ports. As shown by Table 4, both Rotterdam and Hamburg exhibit high levels of digital maturity and strategic integration of cybersecurity within broader governance frameworks. However, differences emerge in the visibility and formalisation of KM practices. Rotterdam describes more explicit forms of knowledge codification and inter-organisational learning, particularly in cybersecurity initiatives, while Hamburg's KM practices remain more implicitly embedded within the disclosure of digital infrastructures and operational processes. Across both cases, KM is consistently under-disclosed as a formal capability, despite being functionally central to DT-enabled decision-making and emissions reduction.

Hence, the results reveal that the selected ports disclose their digitalization, DTs and cybersecurity practices at strategic level, while KM appears mainly through indirect or embedded disclosure evidence. Cybersecurity-related knowledge is publicly represented through collaborative security initiatives, awareness mechanisms, data-sharing practices and digitally enabled coordination, rather than through explicitly institutionalised KM systems. The limited visibility of structured KM practices suggests a disclosure gap between ambitious digital strategies and the knowledge processes needed to support cybersecurity governance, DT reliability and emissions decision-making.

5. Discussion

This study offers insights into how European ports adopting DT disclose cybersecurity and KM practices within the context of the net-zero transition. Regarding the research question, the results suggest that European ports with higher levels of digital maturity increasingly see cybersecurity and KM as mutually supporting capabilities, integrating them into their GHG reduction strategies thereby converging digital innovation, resilience and environmental goals.

The disclosure evidence suggests a possible pathway through which cybersecurity governance, KM mechanisms and DT-enabled workflows may support emissions-relevant decision-making. Cybersecurity-related learning signals may be codified through KM processes and embedded into digital operational routines, contributing to more adaptive and efficient decisions. However, the disclosures do not allow us to assess whether this process is fully institutionalised internally. DT-enabled sustainability may depend not only on technological advancement, but also on the maturity of KM processes that support the capture, sharing and reuse of cybersecurity-related knowledge.

The manual content analysis reveals an increasing disclosure of practices related to data governance, cyber risk management and collaborative knowledge exchange, underscoring their transition toward integrated cybersecurity–KM frameworks. First, the integration of advanced data analytics enhances operational transparency and decision-making by providing deeper insights into port performance (Port of Rotterdam, 2025a, 2025b).

Table 4 Cross-case comparison of Rotterdam and Hamburg ports

Dimension	*Disclosure Evidence* *Port of Rotterdam*	*Port of Hamburg*	*KM interpretation*	*Comparative insight*	*Limits of inference*
Digitalisation and Digital Twin use	■ Data-driven port management systems ■ Digital tools for port call optimisation and traffic management ■ Digital Twin integrating logistics and operational processes	■ SmartPORT digital ecosystem ■ Digital Port Twin used for infrastructure planning and simulation ■ Digital traffic optimisation systems	Public disclosures suggest that both ports represent digital systems as infrastructures for collecting, integrating, and mobilising operational knowledge	Both ports exhibit high levels of digital maturity and rely on digital systems to support operational efficiency	The documents do not allow assessment of how digital knowledge is governed, validated, or reused internally
Cybersecurity governance	■ Cyber resilience framed as strategic priority ■ Participation in the FERM cyber resilience network ■ Internal awareness initiatives (e.g., code of conduct on phishing risks)	■ Cybersecurity addressed mainly through sectoral guidelines ■ References to training and awareness initiatives ■ Alignment with international port cybersecurity recommendations	Cybersecurity-related disclosures suggest mechanisms of knowledge codification, awareness building, and inter-organisational knowledge sharing	Rotterdam shows more explicit governance mechanisms and inter-organisational coordination	The difference between the cases concerns disclosure visibility, not necessarily actual organisational capability
KM-related routines and artefacts	Discloses evidence of knowledge sharing through: ■ cybersecurity collaboration networks; ■ information exchange among port stakeholders; ■ Partial codification of cybersecurity knowledge	Discloses knowledge sharing mainly through: ■ smart-port initiatives; ■ digital infrastructure projects; ■ learning processes embedded in operational digitalisation	KM appears as an embedded and indirect dimension of digital and cybersecurity governance, rather than as a formally disclosed KM system	In both cases, KM-related mechanisms are visible mainly through indirect disclosure evidence	Formal KM structures, repositories, learning protocols, and KM metrics are not clearly disclosed
DT-enabled operational knowledge flows	■ Provides limited information on structured learning cycles, training frequency, KM metrics, and mechanisms for reusing incident-based knowledge ■ KM is mainly inferred from cybersecurity and digital initiatives	■ Provides minimal disclosure of KM governance structures ■ Learning processes remain mostly implicit in digital projects, with limited reference to formal KM reporting	Under-disclosure of KM operationalisation emerges as a key finding across both cases	Both ports frame DT-enabled data flows as enablers of operational coordination and emissions-relevant decisions	The evidence does not demonstrate that these data flows are embedded in formal KM routines or systematic organisational learning processes
Disclosure of KM operationalisation	■ Limited information on structured learning cycles ■ Limited detail on training frequency and KM metrics ■ KM mainly inferred from cybersecurity and digital initiatives	■ Minimal disclosure of KM governance structures ■ Learning processes mostly implicit in digital projects ■ Lack of formal KM reporting	Under-disclosure of KM operationalisation emerges as a key finding across both cases	KM is consistently under-disclosed as a formal capability across both cases	The typology should be read as a disclosure-based heuristic, not as a measurement of actual KM implementation

Source(s): Authors' manual content analysis of the European Ports' Sustainability Reporting and Website Pages (2020–2024)

Second, digitalization is described as a facilitator of collaborative stakeholder engagement and as an essential enabler for the future energy system by improving energy reliability, reducing costs and accelerating the broader energy transition (Port of Rotterdam, 2025a, 2025b). Third, the deployment of digital platforms, e.g. those supporting just-in-time navigation and berth optimisation, is presented as a pathway through which ports may reduce vessel waiting times, improve supply chain predictability and support emissions-relevant operational decisions (Port of Rotterdam, 2025a, 2025b). The concept of port performance includes aspects like reliability, safety and security compliance (Chlomoudis *et al.*, 2024; Yang *et al.*, 2014). The growing integration of digital technologies challenges ports to balance environmental goals with operational reliability and regulatory compliance, emphasizing the need for governance models that can align performance improvement with resilience and sustainability (World Bank, 2021, 2025).

This multifaceted digitalization strategy aligns with the principles of the STS Theory, which emphasize the inseparability of human, technological and organizational dimensions in shaping complex transformations (Bostrom and Heinen, 1977; Troyer, 2017). The findings suggest that alignment across technological, organisational and human elements may depend on the extent to which cybersecurity-derived learning is institutionalised through KM mechanisms and embedded into operational workflows. Hence, knowledge is central to digital infrastructure effectiveness, but its impact depends on its codification, transfer and reuse across organisational and inter-organisational boundaries.

DTs may enable ports to simulate, monitor and optimize operations while ensuring the integrity, availability and confidentiality of critical data streams (Klar *et al.*, 2023). The cases of Rotterdam and Hamburg Ports indicate that DT deployment is disclosed within port environments characterised by technological readiness, as well as organisational commitment to digital innovation and environmental objectives. These conditions suggest that DTs can function as platforms that may support informed decision-making, secure data flows and collaborative knowledge sharing among stakeholders. The results suggest that ports' decarbonization efforts may emerge from the interaction of technological capabilities (DT and data analytics), organizational enablers (KM and governance structures) and environmental pressures (regulatory and stakeholder expectations). Consequently, DTs may function as platforms to support secure data governance, collaborative knowledge creation and adaptive decision-making, thus potentially fostering a socio-technical ecosystem in which cybersecurity and KM jointly contribute to sustainability and resilience. The results confirm that the increasing reliance on digital infrastructures amplifies cyber risks. Hence, cybersecurity readiness is described as a core pillar of port safety and security strategies, and in some cases explicitly included in broader strategic plans. Moreover, cybersecurity measures are complemented by KM initiatives, e.g. workforce training, incident reporting and cross-functional learning, that institutionalize awareness and support continuous adaptation. The IAPH's guidelines promote a cyber-aware culture within the port environment through tailored training, cybersecurity drills and continuous professional development across all functional areas. The analysed disclosure suggests that cyber resilience may depend not only on technical infrastructure but also on organizational learning, human behaviour and a culture of shared responsibility.

These strategies reframe cybersecurity as a shared organizational responsibility requiring a workforce equipped with the necessary understanding of risk indicators, role-based responsibilities and secure digital behaviours. This calls for KM approaches that promote continuous learning, cross-functional knowledge exchange and a culture that prioritizes digital resilience (Shaw *et al.*, 2009). While these results suggest a clear commitment of the selected ports to fostering cyber awareness, the official websites and sustainability reports often lack detailed information on specific training programs, cyber drills or measurable learning outcomes, suggesting a potential gap between strategic intentions and the effective operationalization of KM practices in port cybersecurity governance.

From a legitimacy and stakeholder theory perspective, the findings highlight that disclosures increasingly serve accountability and signalling functions, as ports seek to demonstrate alignment with stakeholder expectations on resilience, transparency and sustainability. However, this study shows that such disclosures vary significantly in their degree of operational grounding. In line with stakeholder theory, value creation in port ecosystems depends on building trust-based relationships with both internal and external actors. Hence, ethical and transparent disclosure practices become essential to meet regulatory demands and to align with broader societal expectations, as emphasized by legitimacy theory. This points to a possible distinction between substantive capability and symbolic legitimacy in disclosure. The authors do not claim to assess substantive capability directly but use the distinction between substantive capability and symbolic legitimacy as an interpretive lens to evaluate the degree of operational detail contained in public disclosures. Specifically, substantive practices may be indicated by the presence of detailed processes, e.g. training routines, incident response mechanisms and knowledge codification practices, which signal the institutionalisation of cybersecurity and KM within organisational structures. In contrast, high-level or generic statements without supporting operational detail suggest a more symbolic orientation aimed at maintaining legitimacy rather than demonstrating actual capability. Importantly, transparent reporting of cybersecurity and KM practices may reinforce the institutional legitimacy of ports by demonstrating accountability, resilience and a commitment to sustainability goals.

In summary, European ports adopting DTs exhibit a growing tendency to integrate cybersecurity and KM as mutually reinforcing enablers of sustainable and resilient governance. The limited visibility of KM operationalisation in the analysed disclosures can be interpreted in two complementary ways. On the one hand, it may reflect a capability gap, whereby ports have not yet fully institutionalised structured learning processes despite advanced digital infrastructures. On the other hand, it may represent a strategic nondisclosure choice, given the sensitivity of cybersecurity-related knowledge and competitive considerations. Since the data set is based on publicly disclosed reports, the analysis does not allow us to determine which explanation prevails. Rather, the evidence points to the possibility that KM under-disclosure may result from insufficient institutionalisation, deliberate nondisclosure or a combination of both.

Regardless of the underlying rationale, the limited visibility of KM operationalisation is analytically relevant because it suggests that, although ports increasingly disclose advanced digital infrastructures, cybersecurity initiatives and DT-enabled governance, the mechanisms through which cybersecurity-related knowledge is codified, shared, reused and embedded into organisational routines remain weakly specified. This points to the under-disclosure of KM as a formal organisational capability, despite its central role in supporting digital resilience and DT-enabled decision-making. Nonetheless, the absence of standardized reporting frameworks continues to limit the comparability and transparency of such disclosures. Developing a coherent, port-specific disclosure model that integrates cybersecurity, KM and DT-enabled environmental indicators would not only strengthen accountability but also enhance stakeholder trust and legitimize sustainable digital transformation across the European port sector.

5.1 Theoretical implications

This study contributes to the emerging literature at the intersection of digitalization and environmental sustainability in the port sector by investigating how European ports disclose cybersecurity and KM practices as part of their decarbonization strategies. Drawing on the STS, KBV, stakeholder and legitimacy theories, the findings provide a multi-theoretical lens to better understand the strategic and operational role of DTs in shaping sustainable and resilient port ecosystems. The STS perspective underscores that digitalization in ports is not solely a matter of adopting technological infrastructures, but rather a process embedded in

the interrelation between technical systems, human competencies and organizational structures (Bostrom and Heinen, 1977; Troyer, 2017). The findings align with recent conceptualizations of DT-enabled ecosystems as socio-technical environments where cyber-physical integration, data analytics and human expertise converge to enhance sustainability performance and adaptive capacity (Klar *et al.*, 2023).

Ports with higher digital maturity implement digital infrastructures to enhance transparency, stakeholder coordination and real-time monitoring. In line with the KBV theory (Alvarenga *et al.*, 2020), the study suggests that digitalization serves as a strategic enabler of knowledge creation and dissemination across the port ecosystem. More specifically, the study contributes by conceptualizing cybersecurity governance not only as a technical safeguard or risk-control function, but also as a potential source of reusable organizational knowledge within DT-enabled environments. This perspective extends KM scholarship by showing that, in digitally intensive and multi-stakeholder infrastructures such as ports, cybersecurity-generated knowledge can become a reusable organisational resource when it is codified, shared and embedded into DT-enabled governance processes. The integration of cybersecurity into port governance frameworks and the growing emphasis on cross-functional training and cyber-awareness campaigns indicate how cybersecurity-related learning signals may be codified, shared and reused through KM mechanisms to support digital resilience. In this sense, the study further clarifies that the reliability of DT-enabled environments depends not only on protecting data through cybersecurity measures, but also on transforming protected data and cybersecurity-related signals into actionable organisational knowledge through KM processes.

This reinforces the view of knowledge as a critical asset for organizational adaptation, especially under conditions of technological and environmental uncertainty. Moreover, by embedding KM into cybersecurity governance, disclosures suggest that ports increasingly frame cybersecurity governance as evolving from reactive risk mitigation toward more proactive and knowledge-oriented approaches, strengthening their capacity to predict, absorb and recover from disruptions (Erbas *et al.*, 2024; Yu *et al.*, 2023). Stakeholder and legitimacy theories are used as supporting lenses to explain why disclosure matters, particularly in relation to increasing stakeholder expectations for transparency, data protection and sustainable performance. Hence, data protection and cybersecurity readiness are acquiring growing importance among port stakeholders, shaping disclosure practices through which ports publicly communicate cybersecurity-related KM processes to demonstrate accountability, credibility and alignment with stakeholder expectations. Finally, by combining insights from STS, KBV, stakeholder and legitimacy theories, this study supports the conceptualization of ports as dynamic STSs where KM-cyber practices operate as complementary mechanisms for maintaining digital resilience, stakeholder legitimacy and environmental integrity.

5.2 Practical implications

Placing KM at the heart of port operations highlights the process by which DT-enabled ports publicly frame cybersecurity signals as knowledge resources that support operational coordination and governance. From a managerial perspective, the introduction of KM indicators in ports' public disclosure could be beneficial to monitor cybersecurity learning processes, e.g. frequency of cybersecurity training sessions, participation rates in awareness programmes, documentation of lessons learned from incidents. Ports could benefit from reporting specific mechanisms through which cybersecurity knowledge is codified, shared and reused, including training routines, participation in awareness programmes, incident-learning processes, knowledge-sharing structures and indicators capturing the reuse of lessons learned across organisational units.

To improve transparency and comparability, port managers could adopt structured disclosure formats that explicitly report cybersecurity training activities, incident-learning

routines, knowledge-sharing initiatives and the role of digital systems in supporting emissions-related decision-making. Finally, the experience of digitally advanced ports offers a roadmap for scaling innovation and capacity-building across the sector. By leading pilot projects, participating in digital corridors and forming knowledge partnerships with different stakeholders, ports could facilitate the diffusion of best practices and support smaller ports in their digital transitions. Establishing cross-functional governance mechanisms, like cybersecurity learning committees or periodic reviews following incidents, could further ensure that cybersecurity insights are systematically integrated into operational and DT-enabled decision-making processes. Policy support, including targeted incentives and technical guidelines, can further amplify these efforts, positioning ports as key enablers of the maritime industry's broader decarbonization and digitalization goals.

5.3 Limitations

This study presents limitations that could be explored by future research. First, the reliance on secondary data, e.g. NFDs, may limit the accuracy and comprehensiveness of the findings. While sustainability reports and official communications provide valuable insights into organisational priorities and strategic orientations, they primarily reflect narrative representations rather than direct observations of internal practices. Therefore, the findings provide insights into how ports publicly represent governance patterns, knowledge processes and digital integration, but they do not allow for definitive conclusions about the actual internal implementation or operational effectiveness of these practices. Furthermore, the limited disclosure of KM operationalisation also restricts the extent to which the study can assess how cybersecurity-related knowledge is codified, shared, reused and embedded into organisational routines. Second, the study concentrates on the most digitally advanced European ports, specifically those with a current DTs, potentially limiting the generalizability of the findings. Ports that have not yet integrated DTs in their systems may exhibit different practices due to varying levels of technological readiness, resource availability or regulatory frameworks. Third, the analysis is geographically confined to the European context, which may not fully capture the diversity of practices adopted by ports in other regions. While Leximancer offers automated and objective insights, the manual content analysis component may introduce interpretative bias. In addition, the absence of uniform reporting frameworks across the analysed ports may have limited the comparability of their disclosures.

6. Conclusions

This study highlights how European ports publicly frame KM as a central component of cybersecurity governance and sustainability-oriented digital transformation within DT-enabled environments. The results suggest that ports disclose varying levels of cybersecurity governance depth and KM maturity, particularly when learning processes are explicitly codified, shared and embedded within DT-enabled operational narratives. A key insight is that disclosures linking KM with digital infrastructures may reinforce narratives of technical capability and stakeholder legitimacy. In ports such as Rotterdam and Hamburg, the disclosures suggest that KM-related mechanisms, transparent data governance and stakeholder engagement may contribute to system resilience and trust, although the extent of their internal operationalisation cannot be directly assessed from public reports alone. However, the limited disclosure of KM operationalisation also indicates that caution is needed in interpreting these findings. Such under-disclosure may reflect insufficient institutionalisation of KM routines, strategic nondisclosure due to the sensitivity of cybersecurity-related knowledge, or both. Accordingly, this study interprets KM under-disclosure as a meaningful disclosure pattern rather than as direct evidence of either organisational weakness or deliberate opacity.

Furthermore, collaborative stakeholder involvement and well-structured KM processes for cybersecurity awareness are crucial for advancing the digitalisation of ports and securing resilient, sustainable maritime governance. In this context, future research should adopt multi-method approaches to triangulate disclosure-based evidence with additional qualitative and quantitative data sources, e.g. interviews, internal documents, operational indicators, incident and business continuity metrics and longitudinal data. This would allow future studies to validate and extend the present findings by assessing not only how cybersecurity governance and KM practices are publicly represented, but also how they are internally implemented, operationalised and developed over time. Extending the analysis beyond European ports and including less digitally mature contexts would also enhance the generalisability of findings and provide comparative insights into different stages of digital and organisational development.

Acknowledgements

The authors would like to thank the Editor-in-Chief, Associate Editor and reviewers for their helpful comments and suggestions, which helped improve the article. This study is an outcome of the "Blue Shipping & Cruise Laboratory" (BSCLab), Department of Law, University of Naples Parthenope, Naples, Italy.

References

Alamoush, A.S., Ölçer, A.I. and Ballini, F. (2022), "Port greenhouse gas emission reduction: port and public authorities' implementation schemes", *Research in Transportation Business & Management*, Vol. 43 No. 100708, pp. 1-18.

Alsehrawy, R., Doukari, O., Kumar, B. and Watson, R. (2022), "A knowledge management strategy for urban digital twins", in *EC3 Conference 2022*, European Council on Computing in Construction, Vol. 3.

Alvarenga, A., Matos, F., Godina, R. and Co Matias, J. (2020), "Digital transformation and knowledge management in the public sector", *Sustainability*, Vol. 12 No. 14, p. 5824.

Bebbington, J., Larrinaga, C. and Moneva, J.M. (2008), "Corporate social reporting and reputation risk management", *Accounting, Auditing & Accountability Journal*, Vol. 21 No. 3, pp. 337-361, doi: 10.1108/09513570810863932.

Beck, A.C., Campbell, D. and Shrives, P.J. (2010), "Content analysis in environmental reporting research: enrichment and rehearsal of the method in a British–German context", *The British Accounting Review*, Vol. 42 No. 3, pp. 207-222, doi: 10.1016/j.bar.2010.05.002.

Bostrom, R.P. and Heinen, J.S. (1977), "MIS problems and failures: a socio-technical perspective. Part I: the causes", *MIS Quarterly*, pp. 17-32.

Calderaro, A. and Craig, A.J. (2020), "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building", *Third World Quarterly*, Vol. 41 No. 6, pp. 917-938, doi: 10.1080/01436597.2020.1729729.

Cheung, K.F., Bell, M.G. and Bhattacharjya, J. (2021), "Cybersecurity in logistics and supply chain management: an overview and future research directions", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 146, p. 102217, doi: 10.1016/j.tre.2020.102217.

Chlomoudis, C., Kostagiolas, P., Pallis, P. and Platias, C. (2024), "Quality, safety, and security systems in the Greek port industry: over twenty years of research, empirical evidence, and future perspectives", *Logistics*, Vol. 8 No. 4, doi: 10.3390/logistics8040098.

Crofts, K. and Bisman, J. (2010), "Interrogating accountability: an illustration of the use of leximancer software for qualitative data analysis", *Qualitative Research in Accounting & Management*, Vol. 7 No. 2, pp. 180-207, doi: 10.1108/11766091011050859.

Cunha, D.R., Oliveira, C.B.M., de Santana Porte, M., Cutrim, S.S. and Pereira, N.N. (2025), "Strategies for decarbonisation in the port and Maritime sector: key challenges and leading ports", *Revista De Gestão Social e Ambiental*, Vol. 19 No. 4, pp. 1-17.

de la Peña Zarzuelo, I. (2021), "Cybersecurity in ports and Maritime industry: reasons for raising awareness on this issue", *Transport Policy*, Vol. 100, pp. 1-4.

de Vicente-Lama, M., Tirado-Valencia, P., Ruiz-Lozano, M. and Cordobes-Madueno, M. (2023), "The impact of sectoral guidelines on sustainability reporting in ports: the case of the Spanish ports", *Maritime Economics & Logistics*, Vol. 25 No. 3, pp. 499-519.

Del Giudice, M., Della Peruta, M.R. and Carayannis, E.G. (2017), "Knowledge management and corporate social responsibility: an integrated framework", *Journal of Knowledge Management*, Vol. 21 No. 5, pp. 1031-1050.

Di Vaio, A., Zaffar, A., Chhabra, M. and Balsalobre-Lorente, D. (2024), "Carbon accounting and integrated reporting for net-zero business models towards sustainable development: a systematic literature review", *Business Strategy and the Environment*, Vol. 33 No. 7, pp. 7216-7240.

Di Vaio, A., Chhabra, M., Zaffar, A. and Balsalobre-Lorente, D. (2025a), "Accounting and accountability in the transition to zero-carbon energy for climate change: a systematic literature review", *Business Strategy and the Environment*, pp. 1-22.

Di Vaio, A., Palladino, S. and Van Engelenhoven, E. (2025b), "Digital twins in port systems and the contribution of GHG accounting: a literature review", *Management Control*, Vol. 2025 No. 1, pp. 1-26.

Di Vaio, A., Van Engelenhoven, E., Raimo, N. and Garofalo, A. (2025c), "Strategic carbon disclosure and accountable efficiency: reporting shipping industry scope 3 emissions", *Business Strategy and the Environment*, Vol. 35 No. 1, pp. 1003-1021, doi: 10.1002/bse.70210.

Dowling, J. and Pfeffer, J. (1975), "Organizational legitimacy: social values and organizational behaviour", *Pacific Sociological Review*, Vol. 18 No. 1, pp. 122-136.

Engstrom, T., Strong, J., Sullivan, C. and Pole, J.D. (2022), "A comparison of leximancer semi-automated content analysis to manual content analysis: a healthcare exemplar using emotive transcripts of COVID-19 hospital staff interactive webcasts", *International Journal of Qualitative Methods*, Vol. 21, doi: 10.1177/16094069221118993.

ENISA (2022), *Cybersecurity Maturity Assessment Framework*, European Union Agency for Cybersecurity.

Erbas, M., Khalil, S.M. and Tsiopoulos, L. (2024), "Systematic literature review of threat modeling and risk assessment in ship cybersecurity", *Ocean Engineering*, Vol. 306, p. 118059.

European Commission (2020), "Mobility strategy", available at: https://transport.ec.europa.eu/transport-themes/mobility-strategy_en (accessed 4 August 2025).

Faleiro, R., Pan, L., Pokhrel, S.R. and Doss, R. (2021), "Digital twin for cybersecurity: towards enhancing cyber resilience", *in International Conference on Broadband Communications, Networks and Systems*, Springer International Publishing, Cham, pp. 57-76.

FERM (2025), "What is FERM?", available at: https://ferm-zeehavens.nl (accessed 5 August 2025).

Freeman, R.E. (1984), *Strategic Management: A Stakeholder Approach*, Pitman Publishing Inc, Boston, MA.

Ghemawat, P. and Khanna, T. (2003), "The nature of diversified business groups: a research design and two case studies", *The Journal of Industrial Economics*, Vol. 46 No. 1, pp. 35-61, doi: 10.1111/1467-6451.00060.

Guthrie, J., Petty, R., Yongvanich, K. and Ricceri, F. (2004), "Using content analysis as a research method to inquire into intellectual capital reporting", *Journal of Intellectual Capital*, Vol. 5 No. 2, pp. 282-293, doi: 10.1108/14691930410533704.

Heilig, L. and Voß, S. (2017), "A science mapping approach to discover the evolution of port research", *Maritime Economics & Logistics*, Vol. 19 No. 1, pp. 106-133.

Higgins, C., Stubbs, W. and Milne, M. (2018), "Is sustainability reporting becoming institutionalised? The role of an issues-based field", *Journal of Business Ethics*, Vol. 147 No. 2, pp. 309-326, doi: 10.1007/s10551-015-2931-7.

Homayouni, S.M., Pinho de Sousa, J. and Moreira Marques, C. (2025), "Unlocking the potential of digital twins to achieve sustainability in seaports: the state of practice and future outlook", *WMU Journal of Maritime Affairs*, Vol. 24 No. 1, pp. 59-98.

IAPH (2021), "IAPH cybersecurity guidelines for ports and port facilities. Version 1.0", available at: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf (accessed 10 August 2025).

Klar, R., Fredriksson, A. and Angelakis, V. (2023), "Digital twins for ports: derived from smart city and supply chain twinning experience", *IEEE Access*, Vol. 11, pp. 71777-71799.

Landrum, N.E. and Ohsowski, B. (2018), "Identifying worldviews on corporate sustainability: a content analysis of corporate sustainability reports", *Business Strategy and the Environment*, Vol. 27 No. 1, pp. 128-151, doi: 10.1002/bse.1989.

Leoni, L., Gueli, G., Ardolino, M., Panizzon, M. and Gupta, S. (2024), "AI-empowered KM processes for decision-making: empirical evidence from worldwide organisations", *Journal of Knowledge Management*, Vol. 28 No. 11, pp. 320-347, doi: 10.1108/JKM-03-2024-0262.

Lozano, R. and Huisingh, D. (2011), "Inter-linking issues and dimensions in sustainability reporting", *Journal of Cleaner Production*, Vol. 19 Nos 2-3, pp. 99-107, doi: 10.1016/j.jclepro.2010.01.004.

Mehmood, M.S., Shahid, M.R., Jamil, A., Ashraf, R., Mahmood, T. and Mehmood, A. (2019), November). "A comprehensive literature review of data encryption techniques in cloud computing and IoT environment", *in 2019 8th International Conference on Information and Communication Technologies (ICICT)*, *IEEE*, pp. 54-59.

Nankya, M., Chataut, R. and Akl, R. (2023), "Securing industrial control systems: components, cyber threats, and machine learning-driven defense strategies", *Sensors*, Vol. 23 No. 21, p. 8840, doi: 10.3390/s23218840.

Neugebauer, J., Heilig, L. and Voß, S. (2024), "Digital twins in the context of seaports and terminal facilities", *Flexible Services and Manufacturing Journal*, Vol. 36 No. 3, pp. 821-917.

Nonaka, I. and Takeuchi, H. (1995), *The Knowledge-Creating Company*, Oxford University Press. Oxford.

Notteboom, T., Pallis, A. and Rodrigue, J.P. (2022), "Digital transformation", in Notteboom, T., Pallis, A., and Rodrigue, J.P. (Eds), *Port Economics, Management and Policy*, Routledge, London.

O'Dell, C. and Grayson, C.J. (1998), *If Only We Knew What We Know: The Transfer of Internal Knowledge and Best Practice*, Free Press, New York, NY.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y. (2018), "Multi-factor authentication: a survey", *Cryptography*, Vol. 2 No. 1, p. 1.

Papa, A., Chierici, R., Ballestra, L.V., Meissner, D. and Orhan, M.A. (2021), "Harvesting reflective knowledge exchange for inbound open innovation in complex collaborative networks: an empirical verification in Europe", *Journal of Knowledge Management*, Vol. 25 No. 4, pp. 669-692, doi: 10.1108/jkm-04-2020-0300.

Port of Hamburg (2021), "IAPH launches cybersecurity guidelines for ports and port facilities as part of industry call to action to digitalize the Maritime transport chain", available at: www.hafen-hamburg.de/en/press1/news/iaph-launches-cybersecurity-guidelines-for-ports-and-port-facilities-as-part-of-industry-call-to-action-to-digitalize-the/ (accessed 6 August 2025).

Port of Hamburg (2025), "SMARTPORT – the intelligent port", available at: www.hamburg-port-authority.de/en/hpa-360/smartport (accessed 8 August 2025).

Port of Rotterdam (2024a), "Rotterdam port introduces geofence for just-in-time sailing", available at: www.portofrotterdam.com/en/news-and-press-releases/rotterdamse-haven-introduceert-geofence-voor-just-time-varen (accessed 5 October 2025).

Port of Rotterdam (2024b), "Code of conduct", available at: www.portofrotterdam.com/sites/default/files/2024-06/code-of-conduct_0.pdf (accessed 5 August 2025).

Port of Rotterdam (2025a), "Digital report 2024", available at: https://publications.portofrotterdam.com/digital-report-2024/cover (accessed 7 August 2025).

Port of Rotterdam (2025b), "Smart infrastructure", available at: www.portofrotterdam.com/en/port-future/smart-infrastructure (accessed 5 August 2025).

Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A. and Yaacob, R. (2023), "Digitalization and cyber physical security aspects in Maritime transportation and port infrastructure", in *Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance*, Springer International Publishing, Cham, pp. 227-248.

Sahoo, S. (2024), "Assessing the impact of stakeholder pressure and green data analytics on firm's environmental performance–understanding the role of green knowledge management and green technological innovativeness", *R&D Management*, Vol. 54 No. 1, pp. 3-20, doi: 10.1111/radm.12602.

Salvi, A., Spagnoletti, P. and Noori, N.S. (2022), "Cyber-resilience of critical cyber infrastructures: integrating digital twins in the electric power ecosystem", *Computers & Security*, Vol. 112, p. 102507.

Schinas, O. and Metzger, D. (2023), "Cyber-seaworthiness: a critical review of the literature", *Marine Policy*, Vol. 151 No. 105592, doi: 10.1013/j.marpol.2023.105592.

Senarak, C. (2024), "Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases", *Maritime Economics & Logistics*, Vol. 26 No. 1, pp. 105-130, doi: 10.1057/s41278-023-00276-8.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers & Education*, Vol. 52 No. 1, pp. 92-100.

Smith, A.E. and Humphreys, M.S. (2006), "Evaluation of unsupervised semantic mapping of natural language with leximancer concept mapping", *Behavior Research Methods*, Vol. 38 No. 2, pp. 262-279, doi: 10.3758/BF03192778.

Steenkamp, N. and Northcott, D. (2007), "Content analysis in accounting research: the practical challenges", *Australian Accounting Review*, Vol. 17 No. 43, pp. 12-25, doi: 10.1111/j.1835-2561.2007.tb00332.x.

Suchman, M.C. (1995), "Managing legitimacy: strategic and institutional approaches", *The Academy of Management Review*, Vol. 20 No. 3, pp. 571-610.

Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J.P., Andrews, W., Harish, A.V., . . . and Jones, K. (2021), "Case study of a cyber-physical attack affecting port and ship operational safety", *Journal of Transportation Technologies*, Vol. 12 No. 1, pp. 1-27, doi: 10.4236/jtts.2022.121001.

Tao, F., Zhang, H., Liu, A. and Nee, A.Y.C. (2019), "Digital twin in industry: state-of-the-art", *IEEE Transactions on Industrial Informatics*, Vol. 15 No. 4, pp. 2405-2415.

Torelli, R., Balluchi, F. and Furlotti, K. (2019), "The materiality assessment and stakeholder engagement: a content analysis of sustainability reports", *Corporate Social Responsibility and Environmental Management*, Vol. 27 No. 2, pp. 470-484, doi: 10.1002/csr.1813.

Troyer, L. (2017), "Expanding sociotechnical systems theory through the trans-disciplinary lens of complexity theory", in Kahlen, J., Flumerfelt, S. and Alves, A. (Eds) *Transdisciplinary Perspectives on Complex Systems*, Springer, Cham, pp. 177-192, doi: 10.1007/978-3-319-38756-7_7.

Tseng, P.H. and Pilcher, N. (2017), "Maintaining and researching port safety: a case study of the port of Kaohsiung", *European Transport Research Review*, Vol. 9 No. 3, pp. 1-11, doi: 10.1007/s12544-017-0250-z.

Uden, L. and He, W. (2017), "How the internet of things can help knowledge management: a case study from the automotive domain", *Journal of Knowledge Management*, Vol. 21 No. 1, pp. 57-70, doi: 10.1108/JKM-07-2015-0291.

UNCTAD (2022), "Building capacity to manage risks and enhance resilience: a guidebook for ports", United Nations Conference on Trade and Development, available at: https://unctad.org/publication/building-capacity-manage-risks-and-enhance-resilience-guidebook-ports (accessed 2 October 2025).

Unerman, J. (2000), "Methodological issues-reflections on quantification in corporate social reporting content analysis", *Accounting, Auditing & Accountability Journal*, Vol. 13 No. 5, pp. 667-681, doi: 10.1108/09513570010353756.

Wang, L. and Li, Y. (2023), "Estimation methods and reduction strategies of port carbon emissions—what literature says?", *Marine Pollution Bulletin*, Vol. 195 No. 115451, pp. 1-17.

Wang, S. and Wang, H. (2019), "Knowledge management for cybersecurity in business organizations: a case study", *Journal of Computer Information Systems*, doi: 10.1080/08874417.2019.1571458.

World Bank (2021), "Port reform toolkit: second edition. Washington, DC: the World Bank", available at: www.worldbank.org/en/topic/transport/publication/port-reform-toolkit (accessed 3 October 2025).

World Bank (2025), "Port reform toolkit", available at: www.worldbank.org/en/topic/transport/publication/port-reform-toolkit (accessed 3 October 2025).

Yang, Z., Wang, J., Bonsall, S. and Fang, Q. (2014), "A new risk quantification approach in port facility security assessment", *Transportation Research Part A: Policy and Practice*, Vol. 59, pp. 72-90, doi: 10.1016/j.tra.2013.10.001.

Yu, H., Meng, Q., Fang, Z. and Liu, J. (2023), "Literature review on Maritime cybersecurity: state-of-the-art", *Journal of Navigation*, Vol. 76 Nos 4-5, pp. 453-466.

Appendix

Table A1 Key constructs and their operationalization

Construct	*Operational meaning in DT-Enabled ports*	*Sources*
Cybersecurity capability	Technical controls aligned with governance, risk, training, and regulatory compliance; routinized and auditable	Cheung *et al.*, 2021; Mehmood *et al.*, 2019; Nankya *et al.*, 2023; Ometov *et al.*, 2018; Progoulakis *et al.*, 2023; Senarak, 2024; Tam *et al.*, 2021
Knowledge management	Systematic codification, dissemination, and reuse of cyber knowledge through artifacts, routines, and simple reuse metrics	O'Dell and Grayson, 1998; Wang and Wang, 2019
DT-enabled optimization	Data-reliant monitoring and planning whose performance depends on the integrity and availability of underlying data streams	de la Peña Zarzuelo, 2021; Klar *et al.*, 2023
Resilience and continuity	Learning-based readiness supported by redundancy, recovery objectives, and continuity planning	Di Vaio *et al.*, 2025a, 2025b, 2025c; UNCTAD, 2022
Stakeholder legitimacy	Credibility that arises when ports demonstrate how secure knowledge flows support environmental and operational goals	Bebbington *et al.*, 2008; Calderaro and Craig, 2020; Papa *et al.*, 2021; Sahoo, 2024

Table A2 Port performance dimensions where KM–cyber link to environmental outcomes

Dimension	*What it captures*	*Where KM-cyber matter for emissions*
Efficiency	Turnaround time, throughput, resource utilization	Codified cyber learning reduces data errors in arrival planning and resource scheduling, which lowers idle time and fuel burn
Reliability	Predictability of services and schedules	Knowledge reuse stabilizes processes after incidents, limiting variability that would Cascade into extra steaming or anchorage time
Safety and security	Protection against accidental harm and intentional threats	Institutionalized training, drills, and post-incident learning reduce disruptions that would otherwise increase energy use and emissions (Chlomoudis *et al.*, 2024; Tseng and Pilcher, 2017; UNCTAD, 2022; World Bank, 2021, 2025; Yang *et al.*, 2014)

Table A3 Reporting architecture: typical evidence and common gaps (with references)

Area	*What credible disclosure looks like*	*Common gap noted in practice*
Cyber–KM artifacts	Named playbooks, threat models, and lessons-learned repositories referenced with dates or versions	Generic statements about "awareness" without identifiable artifacts (Alsehrawy *et al.*, 2022; Uden and He, 2017)
Learning loops	Descriptions of after-action reviews, cross-functional exercises, and how outputs changed procedures	Absence of a traceable link between incident learning and operational changes (Bebbington *et al.*, 2008; Higgins *et al.*, 2018)
Reuse/coverage measures	Simple indicators such as adoption rates, training coverage, near-miss capture or audit findings	No metrics to judge whether knowledge was actually used beyond the originating team
DT–environment linkage	Concrete DT use cases (for example, arrival scheduling or berth optimization) tied to emissions-relevant decisions	High-level claims about "efficiency" without an operational pathway to GHG outcomes (de Vicente-Lama *et al.*, 2023; Di Vaio *et al.*, 2025a, 2025b, 2025c; Homayouni *et al.*, 2025; Notteboom *et al.*, 2022)

Table A4 Operationalization of the 2 × 2 typology

Dimension	*Low*	*High*
Cybersecurity governance depth	Ad hoc or limited references to cybersecurity; mainly technical or compliance-oriented measures; lack of coordination across actors	Structured and strategic approach including monitoring, incident response, governance frameworks, and ecosystem-level initiatives (e.g. port-wide or cross-port collaboration)
KM maturity	Fragmented or implicit knowledge processes; limited evidence of training or knowledge reuse	Systematic knowledge processes including training, knowledge sharing, codification (e.g. procedures, platforms), and integration into DT-enabled workflows

About the authors

Assunta Di Vaio, PhD, is a Full Professor of Business Administration and Accounting Studies at the University of Naples "Parthenope" (Italy). She served as Deputy Director of the Department of Law (2017–2022) and as the Departmental Delegate for Internationalization/International Affairs from 2023 to 2025. Since 2023, she has also held the Delegate for Research role in the same department. She is a member of the university's Gender Equality Plan (GEP) Local Board (since 2022). She earned her PhD in Business Administration from Ca' Foscari University of Venice. She is an expert in carbon accounting, accountability and sustainability reporting, with a research focus on carbon neutrality, compliance and climate change. She is the author of Accounting for Carbon Neutrality and Carbon Accounting for the Sustainable Transition: Accountability, Compliance and Climate Change, both published by Routledge in its Accounting Series. Her research includes managerial and sustainability accounting, carbon and GHG accounting, decarbonization business strategies, sustainability reporting, sustainable development goals (SDGs) disclosure, biodiversity reporting (including the higher education sector and maritime industry), intellectual capital and gender and education issues. She has published in leading ABS-ranked, peer-reviewed accounting and management journals (i.e. JKM, BSE, CSREM, *Journal of Cleaner Production*, Meditari Accountancy Research); several contributions have informed policy-oriented outputs, including citations linked to the *European Commission's Joint Research Center* (JRC), UNESCO and PEMSEA, and some selected studies have been included in the WHO COVID-19 Research Database. She is an active reviewer for major publishers (Elsevier, Emerald, Taylor & Francis, Wiley, SAGE, Springer, and others) and regularly contributes to international conferences. She is an internationally recognized scholar also for her extensive knowledge in shipping, ports and cruise sectors. She has supervised ten PhD students and has been listed in the World Scientist and University Rankings from 2022 to 2025. She has also been included in Stanford University's World's Top 2% Scientists ranking for four consecutive years (2022–2025). In 2026, she was also included in Research.com's Best Business and Management Scientists in Italy 2025/2026 ranking. Her Research.com profile reports a D-Index of 34, 5,672 citations, and 84 publications, based on bibliometric data collected on January 12, 2026, from OpenAlex, CrossRef, and other recognized scholarly data sources. In the 2024 and 2025 editions, she ranked first in Business & Management and second overall at the University of Naples "Parthenope" and was the top female scholar in Italy in SSD ECON-06/A – Business Economics. Her research has also received international recognition, including the 2024 Maritime Policy & Management Best Published Manuscript Award. She has authored more books on Accounting for Carbon Neutrality and Carbon Accounting (Routledge) and contributes to SEA-EU 2.0 ("European University of the Seas") as an expert member and Co-Lead of Task 1.4. She has supervised ten PhD students and has undertaken a visiting activity at UCL's Quantitative and Applied Spatial Economic Research Laboratory (QASER), University College London (UK). Assunta Di Vaio is the corresponding author and can be contacted at: susy.divaio@uniparthenope.it

Elisa Van Engelenhoven, PhD, earned her doctorate in Law and Economic-Social Institutions: regulatory, organizational and historical-evolutionary profiles at the University of Naples "Parthenope," Italy. Her research includes sustainability disclosure and reporting, GHG accounting, sustainability practices and performance, digitalization, SDGs, especially SDG7, SDG14 and SDG15. These topics have been explored in the fields of electricity, shipping, cruise and higher education sectors. She specializes in using software for content analysis, focusing on examining themes and concepts disclosed in sustainability reporting. Her work

has been published in the Environment, Development and Sustainability Journal by Springer Nature, "Rivista Italiana di Ragioneria e Economia Aziendale", "Business Stretegy and the Environment" and "Business Development" by Wiley, some of her research is currently under review in peer-reviewed journals. Her chapter on the role of the Higher Education Sector in Italy in halting biodiversity loss is about to be published in one of Taylor & Francis' series. She frequently participates in seminars on sustainability accounting and qualitative methodologies. Recently, she has been speaker at the first edition of the international scientific and multidisciplinary conference "Being Sea-EU" in Malta, as well as at the inaugural RIREA workshop in Italy. Elisa is a member of the "Blueshipping & Cruise Lab" (BSCLab) at the Department of Law, University of Naples "Parthenope," Naples, Italy.

Anum Zaffar, PhD, is a winner of a one-year research grant at the University of Naples "Parthenope," Naples (Italy) on measuring and reporting SDGs and decarbonization processes in the shipping industry. She is PhD in Law and Economic-Social Institutions: regulatory, organizational and historical-evolutionary profiles. She is the winner of the International Foreign PhD scholarship. She won the University merit scholarship in her master's in public administration (2012) and MS in Accounting & Finance (2019) and won a merit Laptop under the Youth Development Scheme run by the Government of Pakistan (2011). She remained associated with the faculty of two Women Universities of Pakistan i.e. Fatima Jinnah Women University, Pakistan and Rawalpindi Women University, Pakistan. Her research field includes decarbonization disclosure, responsible innovation and gender equality in the accounting and accountability models; digitalization and renewable resources; intellectual capital and knowledge management in the decarbonization disclosure framework; gender equality and SDGs practices in shipping, cruise, and port industry; carbon accounting and integrated reporting; biodiversity and higher education sector. In this research she explored more SDGs, i.e. SDG1, SDG4, SDG7, SDG8, SDG15, SDG17. She has a good knowledge of Systematic Literature Review methodology. Her first study on decarbonization issues in the shipping industry has been published in *Journal of Shipping and Trade*. Her other articles have been published in the *Journal of Intellectual Capital* (Emerald Publisher) and the *Business Strategy and the Environment Journal* (Wiley Publisher). Her chapter entitled "Carbon and Decarbonization Disclosure: Role of Responsible Innovation in Adoption of Artificial Intelligence of Things towards SDGs" has been published in the book "Artificial Intelligence of Things for Achieving Sustainable Development Goals" which is to be published in "Lecture Notes on Data Engineering and Communications Technologies", Springer. She regularly attends seminars and conferences on these issues. She attended the annual conference by the International Association Maritime Economics (IAME) on decarbonization technology responsibility, gender equality and sustainable business models in the shipping field. She regularly attends as a speaker at the International Conference on New Business Models. She has been a visiting scholar at the University of Castilla-La Mancha, Spain to depth decarbonization, digitalization and renewable energy issues in the sustainability reporting systems. Several of her book chapters are currently undergoing review in prestigious double-blind peer-reviewed series published by Elsevier and Taylor & Francis. Anum is a member of the "Blueshipping & Cruise Lab" (BSCLab) at the Department of Law, University of Naples "Parthenope," Naples, Italy.

Gabriella D'Amore, PhD, is an Associate Professor of Business Administration at the University of Naples Parthenope, Italy. She is qualified as a Full Professor in the same scientific field and serves as Associate Editor of the international journal Environment, Development and Sustainability. Her research fields include governance, performance measurement and sustainability assessment and reporting of companies' environmental and social impacts, especially in the utilities sector. Her research has been published in books and top-tier peer-reviewed journals. She has been a visiting scholar at the Department of Community, City and Regional Planning at Cornell University, NY, USA.