From Compliance to Resilience: A Practitioner-Led Cyber Security Management Framework for LNG and Tanker Fleet Operations Aligned with USCG and IMO Regulatory Requirements

Captain Anand Dubey[1], Hazem Abu-Adaiq[2*]

[1] Dev Nagari College, Meerut, Uttar Pradesh, India.
(ananddby@yahoo.com)

[2] Cybersecurity and Cloud Computing, Faculty of Information Technology,
Applied Science Private University, Amman, Jordan.
(h_abuadaiq@asu.edu.jo)
ORCID: 0000-0002-9700-0968

Corresponding Author:

Captain Anand Dubey[1*]
Email: ananddby@yahoo.com

Abstract: The rapid digitalization of LNG carrier and petroleum tanker operations has substantially expanded the cyber-attack surface of some of the world's most consequential maritime assets, yet a persistent gap remains between the intent of international regulatory instruments and their operational implementation at fleet management level. Drawing on thirteen years of HSEQ/Tanker Operation management experience within LNG and tanker fleets, active participation in SIRE 2.0 development, and direct involvement in Cyber Security Management Plan (CSMP) drafting at Vice President level within a major LNG shipping group, this paper presents a practitioner-developed CSMP framework derived from a three-layer qualitative analysis: systematic regulatory mapping across IMO, USCG, and NIST instruments; operational framework construction; and a structured gap analysis comparing regulatory requirements against operational practice. The framework identifies five critical implementation gaps, including the OT/IT convergence challenge, entirely unaddressed in all current regulatory instruments, and proposes a five-component, scalable CSMP architecture embedded within the existing ISM Code Safety Management System. To the authors' knowledge, this is the first practitioner-led, vessel-type-specific CSMP integrating IMO, USCG, and NIST requirements into a single executable operational architecture for LNG and tanker fleet environments. Given the centrality of US LNG export terminals, Cameron LNG, Sabine Pass, and Freeport LNG, to US energy security and foreign policy, the framework carries direct significance for USCG regulatory development, domestic LNG terminal operators, and national critical infrastructure protection.

Keywords: Maritime Cyber Security; LNG Fleet Operations; Tanker Safety Management; SIRE 2.0; USCG Cyber Strategy; IMO MSC.428(98); Cyber Resilience; OT/IT Convergence; Safety Management Systems; CSMP Framework

Introduction

The adoption of digital technology across maritime operations has accelerated markedly over the past decade, fundamentally transforming the operational architecture of vessels that carry the world's most strategically sensitive cargoes. (Kalogeras, 2023). Liquefied natural gas (LNG) carriers and petroleum tankers, the assets whose safe and reliable running are the foundations of energy security in the world, are now reliant upon a multi-layered ecosystem of integrated operational technology (OT) and information technology (IT) systems. (Marroni et al., 2023): electronic chart display and information systems (ECDIS), cargo management systems (CMS), emergency shutdown (ESD) systems,

re-liquefaction plant controls, automated mooring interface, and satellite communications infrastructure, which are emerging to form the digital backbone of modern gas carrier and tanker operations (Afenyo & Caesar, 2023; S. Gopinath et al., 2025). This transformation has delivered measurable gains in navigational precision, cargo management efficiency, and regulatory compliance monitoring, while simultaneously introducing systemic cyber vulnerabilities that the sector has been structurally slow to address at the operational level, and that no existing regulatory instrument has resolved with the prescriptive specificity that LNG and tanker ship managers require..

The manifestation of this weakness is empirical and regulatory. In the period between 2020 and 2024, the maritime industry had to endure a series of high-profile cyber-attacks, such as the ones on the IMO itself and on CMA CGM in 2020 and the breaches of Euronav systems in 2021 and the myriad of undisclosed OT-system attacks that DNV, in its annual surveys of maritime cyber priorities, revealed that no level of the maritime industry is immune to cyber-attacks (DNV, 2023). The regulatory response has been substantive yet operationally non-prescriptive. Resolution MSC.428(98) of the International Maritime Organization placed the onus on Safety Management Systems (SMS) to include an appropriate response to the maritime cyber risks by January 2021, but with guidance provided in MSC-FAL.1/Circ. 3/Rev.1 (2021). The Maritime Cyber Strategy 2021 of the United States Coast Guard has identified three pillars of strategy: a cyber-ready workforce, resilient systems, and interagency partnerships, but expressly acknowledges the existence of critical maritime infrastructure, such as LNG export terminals and tankers involved in the latter, as assets of national security interest (Tsailas, 2025). The 2023 Ship Inspection Report Program 2.0 (SIRE 2.0) provided by the Oil Companies International Marine Forum (OCIMF) added structured questions about cyber security assessment to the tanker vetting process, making commercial non-compliance not only a regulated but also a financial risk (Grbić et al., 2018; Pavić et al., 2024).

Regardless of this regulatory ambition convergence, there is still a fundamental gap in operational ambition. The structures developed by the IMO, USCG, and the National Institute of Standards and Technology (NIST) each represent what cyber resilience must accomplish, yet they each offer little in the way of prescriptive advice regarding how fleet operators that operate LNG carriers and tankers are expected to incorporate these specifications into the currently implemented safety management systems. (Kim & Lee, 2025). BIMCO Cyber Security Guidelines (4th Edition, 2021) is the most substantive attempt to address this gap to date made by the industry, but it is aspirational in nature, specifically indicating that ship-type-specific advice was outside its remit, which is directly where this research paper aims to fill the gap (Kalogeras, 2023). As Progoulakis et al. (2021) noted that the disconnect between regulatory articulation and operational implementation in maritime cybersecurity constitutes not merely a challenge of regulatory ambition. Still, fundamentally an issue of operational translation, a finding the current study confirms and extends to the specific technical and organizational environment of LNG and tanker fleet management.

This discontinuity has both operational and national implications. The commissioning of new export infrastructure has substantially expanded US LNG capacity over the past five years, with Cameron LNG representing one such addition. Sabine Pass, Freeport LNG, and Corpus Christi LNG are all key hubs of the national energy and foreign policy infrastructure of the United States (Bolbot et al., 2022; Marroni et al., 2023). Maritime critical infrastructure, consisting of LNG facilities and vessels that serve them, is specifically listed as the area of national security concern in the 2021 Maritime Cyber Strategy of the USCG. However, there exists no LNG-specific maritime cyber guidance that has been given by the USCG, the Federal Energy Regulatory Commission (FERC), or any other US federal regulatory agency, and it creates a significant policy gap precisely at the nexus of shipboard cyber vulnerability and national energy security exposure (Melnyk et al., 2025).

Since 2020, academic literature on maritime cybersecurity has increased significantly, though it has mostly taken the form of a broad regulatory analysis. (Kayişoğlu et al., 2022; Melnyk et al., 2025) or a technical-focused vulnerability assessment framework (Putra et al., 2023; Svilicic et al., 2019; Tam & Jones, 2019). The particular collision of LNG carrier activities, OT/IT convergence weaknesses within the gas carrier setting, frontline managerial production of CSMP, and USCG policy makers had not been debated within the prior literature, leaving the ship managers, flag state regulators, and USCG

policy developers lacking an operationally based, vessel-type receptive framework (Bolbot et al., 2022; Kim & Lee, 2025).

This paper addresses a single overarching research question: Do current international and US maritime cyber security frameworks provide operationally sufficient guidance for LNG and tanker fleet managers, and what practitioner-led CSMP architecture is needed to close the gap between regulatory compliance and genuine operational cyber resilience?. This study makes three distinct contributions. Theoretically, it applies resilience engineering and high-reliability organization theory to the maritime cyber context, demonstrating that compliance-oriented regulatory frameworks are structurally misaligned with the adaptive capacity requirements of high-consequence vessel operations. Practically, it produces the first operationally executable, LNG-specific CSMP architecture, including the novel Ship-Shore Cyber Interface Register, that ship managers can implement within existing SMS structures without additional regulatory mandates. At the policy level, it provides the first systematic alignment of IMO, USCG, NIST, and SIRE 2.0 requirements against ten operational domains, identifying the complete absence of OT/IT convergence guidance as the most critical regulatory gap facing US LNG export terminal operations and national maritime security.

Literature Review

2.1 The Evolving Maritime Cyber Threat Landscape

Definitions of cyber threats facing maritime operations have significantly changed since the sector is now operationally vulnerable following the 2017 NotPetya cyberattack on the Maersk Line. Cyber incidents involving maritime have increased in frequency, sophistication, and scope of operation since 2020, not only on business IT but also in OT environments controlling vessel safety functions. A report by the Maritime Cyber Priority Report (2023) by DNV recorded a great rise in OT-system incidents, where 25 per cent of professionals in the maritime industry reported cyber events on operational technology in the past three years, an incidence that DNV itself found to be grossly underreported due to the established records of underreporting. (Mäurer et al., 2022; Oluwoye & Oyedeji Oluwoye, 2020). The ransomware attack of 2020, which affected the global bookings and operational data flow of the company weekly and the coordinated attack on the IT infrastructure of the IMO itself, helped to realize that no level of the maritime system has a barrier to the infiltration of information by cybercriminals. (DNV, 2023; Kechagias et al., 2022).

The threat taxonomy which LNG and tanker operations have to deal with is more pronounced and more consequence-sensitive than that of general cargo or container shipping, as the systems involved in these operations are required to ensure the physical safety of the dangerous shipment. The disadvantages of ECDIS, such as vulnerability to GPS spoofing, manipulation of chart data, and alteration of the route, are reported on various vessels (Androjna et al., 2021; S. Gopinath et al., 2025).

The culture of under-reporting that infuses the disclosure of maritime cyber incidents adds to the problem of proper threat characterization of the threat landscape. Hopcraft et al. (2023) found the unwillingness to report cyber incidents by organizations to be reported as one of the key obstacles to collective reduction of maritime cyber risks. They explained that such obstacles were concentrated mostly around the consideration of the outcomes of vetting inspections in the context of the SIRE 2.0 and TMSA regimes. In the survey provided by Marroni et al. (2023), the data indicated that reported incidents were less than 40 per cent of the real-world occurrences, a structural information gap, which interrupts the loops of feedback on regulation that would ordinarily have been present at an industry level. The present study identifies this dynamic of under-reporting in the gap analysis as Gap 4. It considers it a design constraint to the incident detection and response part of the proposed framework.

2.2 Regulatory Frameworks and Their Operational Limitations

There has been significant progress in the development of the international regulatory framework of maritime cybersecurity since the introduction of the SMS-integration requirement in IMO Resolution MSC.428(98) in 2017 and guidelines supporting the mandatory establishment in MSC-FAL.1/Circ. 3/Rev.1 in 2021. The conceptual architecture of the framework reflects the five functions of the NIST Cybersecurity Framework, which are Identify, Protect, Detect, Respond, and Recover.

Although this correspondence is theoretically consistent, it has never been turned into operational prescriptiveness. Using the maritime cybersecurity policy as the context of the system dynamics modelling, Putra et al. (2024) made a conclusion that the principle-based regulatory framework generates loops of feedback that merit compliance documentation presented without operational resilience, as there are no performance metrics within which operationally feasible substantive assessment can take place. This dynamic, in which regulatory instruments incentivise the appearance of compliance rather than its substance, has been identified as a structural feature of principle-based governance regimes across sectors. Patyrykin (2025); Sarfaraz (2025), examining ESG rating frameworks in the insurance sector, demonstrated that symbolic compliance and genuine accountability diverge systematically when regulatory instruments lack prescriptive performance standards, a finding that mirrors the maritime cyber regulatory environment at the operational level. A study of the discrepancy between flag state applications of the requirements of the IMO and the port state inspection practice, conducted by Melnyk et al. (2025) revealed that the lack of prescriptive standards makes both the flag and the port state inspection practice inconsistent and ineffective. The USCG Maritime Cyber Strategy (2021) is a more operationally oriented tool than its IMO counterpart, specifically in its identification of maritime critical infrastructure as a domain of national security and its expression of particular workforce, systems and partnership pillars (Tsailas, 2025). Nevertheless, the technology-neutral strategy of the USCG strategy, suitable due to its wide-ranging jurisdictional set, leaves a vessel-type divide between the essentially different OT architecture of an LNG carrier and a container ship, as Dimakopoulou and Rantos (2024) demonstrated in its analysis of the adoption of NIST CSF to marine transportation systems.

SIRE 2.0 inspection regime was introduced in 2023 and added a new business facet to maritime cyber security compliance, which is an addition to the regulatory paradigm that is still not captured in the current literature (Pavić et al., 2024). The series of Q.7.1 questions demand recorded proof of cyber security governance, CSMP execution and crew awareness which, to a degree, makes the formation of commercial pressure that demands conformity regardless of regulatory pressure established by IMO and USCG tools. However, SIRE 2.0 needs CSMP documentation with no minimum CSMP content indicator, which presents a dilemma: the vetting mechanism creates the commercial pressure needed to improve cyber security but not the operational architecture through which the latter is becoming consistent and measurable.

2.3 LNG and Tanker-specific Cyber Vulnerabilities

The OT systems most vulnerable to intrusion are safety critical in nature, which sets the cyber vulnerability profile of the LNG carriers and tankers apart from that of other ships. In their in-depth survey of vulnerabilities in the cyber-physical systems that directly relate to tankers and LNG carriers, Bolbot et al. (2019) verified the main role that the process of OT/IT integration plays in transforming low-consequence breaches of IT networks into high-consequence safety events. Their consideration showed that it is technically possible to have lateral migration of administrative IT networks to the OT safety systems within the current integrated vessel network designs, the result of which has streamlined devastating impacts especially on LNG carriers whose OT networks control reagents of cryogenic cargo handling, gas detection, and emergency closures.

Enoch et al. (2021) used attack graph analysis to demonstrate that a maritime vessel OT/IT infrastructure could take three to four lateral moves in a publicly available network interface to a safety-critical system by using an integrated network architecture. Applied to the LNG carrier situation, this implies that when a phishing email is opened on the administrative network of a ship, the most frequent first attack vehicle reported in the case of maritime cyber-attacks, a practical attack route to the cargo management system can be obtained without any special maritime cyber-attack solution (Bolbot et al., 2022).

Marroni et al. (2023) offered the safest security integrated evaluation of LNG carrier cyber risk that has been up to date recorded in peer review literature in which bow-tie analysis is used to evaluate the effects of cyber-induced ESD failure experienced during the process of loading LNG cargo. Their discovery that a cyber-induced ESD malfunction upon loading at a major terminal could have comparable outcomes as a physical attack, such as the uncontrolled release of LNG through cloud of

vapor, provides the national security aspects of LNG vessel cyber security in terms that the current regulatory framework fails to address at all. Longo et al. (2024) based on the industrial control systems security principles identified the maritime OT/IT convergence environment, and as assumptions inherent in existing maritime cyber guidance were formed based on a conceptual framework, which does not mirror the technical reality of a modern gas carrier and tanker operation.

2.4 Theoretical Framework: Resilience Engineering and Safety Management System Integration

The foundations of this study are resilience engineering paradigm and its implementation in the management of maritime safety. Hollnagel has introduced resilience engineering, developed by a team of workers in two decades of work in high-consequence industries, that suggests that the safety of a complex sociotechnical system is not achieved mainly by the absence of failures in the system but by building organizational adaptive capacity, the ability to modify how the system functions when conditions change, both anticipated and unanticipated before, during, and after to continue the needed operations (Hollnagel, 2017).

This framework is a crucial theoretical change to the compliance-based model that underlies most of the maritime cyber regulatory tools, of trying to stop bad events happening through documentation and procedural compliance to the requirement, rather than building the organizational face to absorb, adapt, and recover to the cyber incidents that are bound to happen in a complex, digitally integrated operating environment. The high-reliability organization (HRO) theory of Weick and Sutcliffe (2001) offers a theoretical perspective that is highly relevant in the context of the maritime industry. The theory of HRO has proposed five attributes of organization that are safely functioning within high-consequence environments: preoccupation with failure (active search of anomalies before they accumulate), unwilling to simplify (resistance to oversimplification of complex risk signals), sensitive to operations (sustained situational awareness in the sharp end), committed to resilience (capability to detect, contain, and recover errors), and deferential to expertise (authority moving to those with knowledge despite their level).

Furthermore, when applied to the management of maritime cyber security, HRO theory would be accurate predictors of the identified gap modes of organizational failure of the present study, i.e. the incident reporting culture gap terms the organizational context where the culture of preoccupation with failure is not achieved, as the reporting mechanisms equated the learning-focused near-miss capture process with the regulatory and commercial exposure. It is the model of compliance documentation the current SIRE 2.0 and IMO auditing model encourages to the emergence of cyber security preparedness without confirming the operative capacity the HRO theory recognizes as constituent of real organizational dependability (Weick & Sutcliffe, 2001).

Both the resilience engineering and the HRO frameworks facilitate the re-understanding of the concept of maritime cyber security management as a compliance-focused, documentation-oriented model through a resilience-focused, operationally embedded model whereby the Safety Management System becomes a living operational tool that matures and maintains operational capability along five areas, namely asset knowledge, threat awareness, access governance, incident responsiveness, and interface management. This redefinition is operationalized directly within the five-elements frameworks of CSMP created in the results section of this study, in which the five components are to be developed not only to meet a regulatory standard but also to create an organizational capability that will contribute to the adaptive capacity foundation of operational reliability in high-consequence systems identified by resilience engineering.

2.5 Synthesis and Research Gap

The literature reviewed establishes a coherent and consistently identified research gap, which can be categorized across three distinct dimensions. Academically, while the theoretical foundations of maritime cyber resilience are well-established (Hollnagel, 2017; Weick & Sutcliffe, 2001), and the regulatory framework has evolved greatly since 2020 (Bekiashev & Serebriakov, 1981; *USCG CYBER STRATEGIC OUTLOOK*, 2021), there is no practitioner-based, vessel-type-specific CSMP framework to cover LNG and tanker operations that combines IMO, USCG, and NIST requirements into an integrated framework. The importance of unified and integrative frameworks in addressing multi-dimensional

system challenges has been emphasized across engineering and decision sciences (Abualhomos et al., 2025).

The present study fills this gap across three dimensions. Academically, no published study has produced a practitioner-derived, vessel-type-specific CSMP framework integrating IMO, USCG, and NIST requirements for LNG and tanker operations; existing contributions are either theoretically oriented or generically applicable across vessel types. Operationally, ship managers lack prescriptive, SMS-integrated guidance for implementing cyber resilience in practice, particularly for the OT/IT convergence challenge that is unique to modern LNG carrier network environments and entirely unaddressed across all current regulatory instruments. At the policy level, the complete absence of LNG-specific maritime cyber guidance from the USCG, FERC, or IMO leaves a critical regulatory void at the intersection of shipboard cyber vulnerability and US national energy security, which this study directly addresses.

Methodology

3.1 Research Design and Justification

The study follows a mixed-method research approach, utilizing qualitative and framework-development research. Three methodological choices explain why a qualitative approach was chosen. To begin with, the investigated phenomenon, the adaptation of marine regulatory requirements on cyber security into the working fleet management practice is interpretive and context-bounded, and its quantification requires a considerable amount of operational validity. Such adaptation challenges are often influenced by organizational and behavioral factors affecting technology adoption, including user readiness, training exposure, and perceived utility (Alkasasbeh et al., 2025). The organizational dynamics underlying technology adoption resistance are equally relevant to embedding new cyber security frameworks within established maritime management cultures. Research on strategic deployment of digital tools in organizational settings has consistently demonstrated that misalignment between new system capability and existing organizational structures is a primary driver of implementation failure (Patel & Patyrykin, 2015). Similarly, the broader literature on normative volatility and organizational culture demonstrates that institutions operating under shifting ethical and behavioral expectations face compounded resistance when introducing governance instruments that demand behavioral change from established professional communities (Patyrykin, 2025). The CSMP framework is therefore deliberately designed for integration within the existing ISM Code SMS architecture rather than as a parallel management system, recognizing that framework-to-structure alignment is the critical determinant of whether new governance instruments become operational practice or remain documentary compliance artifacts.

Second, the primary data source for the framework construction layer is practitioner expertise accumulated over thirteen years of direct HSEQ management within LNG and tanker fleet environments, hands-on CSMP drafting, and active participation in the SIRE 2.0 development process. This constitutes a form of tacit operational knowledge that qualitative framework-development methodology is best equipped to systematize, as argued by established interpretive research traditions in safety management and organizational studies. Similar modeling-driven approaches have been successfully applied in complex engineering systems to translate theoretical constructs into operationally applicable frameworks (Aboshighiba et al., 2025).

The use of practitioner knowledge as a primary data source is a recognized and academically legitimate approach in applied maritime research, provided it is subjected to systematic analytical structure and multi-source triangulation, both of which are explicitly incorporated into this study's three-layer design. Third, the maritime cyber security domain lacks the standardized, longitudinal incident data needed to support statistically-based vulnerability quantification; the under-reporting culture documented in Section 2.1 means available quantitative data is structurally incomplete for population-level inference. To ensure reproducibility and reliability, the framework development process follows a structured sequence: Layer 1 produces a documented regulatory mapping matrix replicable by any researcher with access to the same public instruments; Layer 2 framework

components are explicitly mapped to regulatory requirements and SIRE 2.0 criteria, enabling external verification; and Layer 3 gap ratings are cross-referenced against published survey data rather than resting on practitioner judgement alone. This structured sequence ensures that another researcher following the same protocol with equivalent practitioner access would arrive at substantively equivalent framework outputs.

3.2 Analytical Approach/Framework Development Process

The methodology is divided into three consecutive steps of the analysis, which make up the framework development process. Step 1 is systematic regulatory mapping systematic content analysis of all primary regulatory and industry guideline documents bearing on maritime cyber security, to identify (a) the requirements each instrument has on ship managers and fleet operators, (b) how requirements are articulated to reflect operational specificity, and (c) points of coincidence and divergence between requirements by the operational requirement-level instruments. Comparative analytical approaches are widely used to evaluate system performance differences and identify optimal configurations across complex domains (Adaileh et al., 2025).

The second step is the framework construction by practitioners: mapping operationalization of regulatory requirements into a vessel-type-specific CSMP architecture, based on the available documented experience in the field of LNG and tanker HSEQ management, CSMP development, participation in the SIRE 2.0 and interaction with oil major vetting processes over the course of over 13 years. Step 3 is gap analysis: an organized session where the regulatory requirements determined in Step 1 are compared with the realities of operations of LNG and tanker fleet management as perceived by practitioner experience, published survey results, and as estimated using SIRE 2.0 assessment results.

Table 1:Data Sources Employed Across the Three Analytical Steps

Data Source Category	Specific Sources Used	Analytical Step	Justification for Inclusion
IMO Regulatory Documents	IMO MSC-FAL.1/Circ.3/Rev.1 (2021); Resolution MSC.428(98) (2017); ISM Code (2018 consolidated edition); MSC-FAL.1/Circ.3 original (2017)	Step 1, Regulatory Mapping	Primary international regulatory source establishing the SMS-integrated cyber risk management obligation; foundational to framework alignment and gap identification.
USCG Strategy & Regulations	USCG Maritime Cyber Strategy (2021); 33 CFR Parts 101–106 (Maritime Transportation Security Act regulations); USCG Cyber Strategic Outlook (2023); DHS National Maritime Cybersecurity Plan (2021)	Step 1, Regulatory Mapping	Defines US-specific obligations for vessels and port facilities; essential for aligning CSMP notification thresholds with USCG requirements; establishes national security context for LNG cyber vulnerability.
NIST Framework Documents	NIST Cybersecurity Framework 2.0 (2024); NIST SP 800-82 Rev.3, Guide to OT Security (2023); NIST SP 800-37 Rev.2, Risk Management Framework (2018)	Step 1, Regulatory Mapping	Provides technically granular risk management architecture; cross-referenced for OT-specific security controls applicable to LNG carrier network environments.

Industry Guidelines	BIMCO Cyber Security Guidelines 4th Ed. (2021); OCIMF SIRE 2.0 Technical Specifications (2023); OCIMF TMSA 3 (2021); IEC 62443-3-2 Security Risk Assessment (2020)	Steps 1 and 2	Industry self-regulatory instruments bridging IMO requirements and operational practice; SIRE 2.0 directly shapes vetting exposure and commercial cyber compliance pressure for LNG and tanker operators.
Practitioner Experience Documentation	13+ years HSEQ management records; authored CSMP documentation (anonymized per professional obligations); SIRE 2.0 development participation records; LNG fleet operational procedures documentation; mooring analysis and SSCS records for LNG vessels; ISM/ISPS audit records	Step 2, Framework Construction	Primary practitioner data source providing operational validity and vessel-type-specific grounding unavailable in academic or regulatory literature; constitutes the study's central methodological contribution.
Published Incident & Survey Data	DNV Maritime Cyber Priority Report (2023); BIMCO/Thetius Cyber Security in Shipping Survey (2022); IMO cyber incident reporting summaries (2021–2024); ENISA Port Cybersecurity Report (2023)	Step 3, Gap Analysis	Provides empirical grounding for gap severity ratings; cross-referenced against practitioner observations to validate gap identification and confirm prevalence across industry.
Peer-Reviewed Academic Literature	Systematic database search: Scopus and Web of Science; date range 2020–2026; search terms: 'maritime cyber security', 'LNG cybersecurity', 'tanker OT security', 'IMO cyber compliance', 'maritime cyber resilience', 'SIRE inspection cyber'	All Steps	Academic literature provides theoretical framework (resilience engineering; HRO theory) and comparative context for discussion; search yielded 312 results; 44 papers included after title/abstract and full-text screening.

Note. Regulatory documents accessed in their most current published versions as of December 2024. Practitioner documentation anonymized in accordance with professional obligations; the author's professional affiliations and experiences are documented in the author note. Academic literature search conducted November–December 2024; 312 results yielded, 44 papers included after title/abstract and full-text screening against inclusion criteria (peer-reviewed; published 2020–2026; directly relevant to maritime cyber security, LNG/tanker operations, or resilience engineering).

Table 1 yields four analytically significant insights. First, all three regulatory instruments converge on the NIST Cybersecurity Framework's five functions conceptually, but diverge entirely at

the level of operational prescription, producing a compliance-execution void that this study is designed to close. Second, IMO Circular MSC-FAL.1/Circ.3/Rev.1 provides the broadest international mandate but the lowest operational specificity across all ten domains, delegating all implementation detail to ship managers without prescribed outcomes or minimum performance standards. Third, the USCG Maritime Cyber Strategy, while more operationally focused on its incident notification and port interface provisions, remains technology-neutral in ways that make it vessel-type blind, applying identical requirements to an LNG carrier and a bulk carrier despite fundamentally different OT architectures and safety consequence profiles. Fourth, and most critically, OT/IT convergence is the single domain of complete regulatory silence across all four instruments, representing the most consequential unaddressed vulnerability in modern LNG carrier operations. To address the validation limitation inherent in qualitative framework-development research, each CSMP component is explicitly benchmarked against SIRE 2.0 Q.7.1 inspection criteria, the most current commercial vetting standard applied to LNG and tanker operators, providing a form of expert-criterion validation that confirms the framework satisfies both regulatory requirements and the inspection expectations of oil major vetting regimes.

3.3 Validity and Limitations

The framework was tested in three ways simultaneously. First, regulatory triangulation triangulated the requirements between IMO, USCG, NIST CSF 2.0 and BIMCO GL4 tools, so that none of the gaps is identified based on the framework of a single tool only; all gaps identified in Table 3 are seen in all four frameworks, not only one. Second, practitioner-literature triangulation cross-referenced all five CSMP components with peer-reviewed evidence on maritime cyber vulnerabilities and HRO theory, to enable independent evidence to support the operational experience of the author. Third, criterion-based validation measured all component specifications against SIRE 2.0 Q.7.1 inspection requirements; the live commercial vetting standard applied to LNG and tanker operators by oil majors throughout the world, which established that the framework not only met regulation standards but also met contemporary inspection standards as well. It is a recognized criterion-based approach in applied qualitative research in which longitudinal field testing is not possible yet. The personal experience of the author with the development of SIRE 2.0 and drafting of CSMP on behalf of a leading LNG fleet operator gives the practitioner power within the framework of which the consistency of outputs of the frameworks with the legitimate needs of the actual process of vetting can be estimated.

Results

The results put forth three findings that were obtained from this study. First, systematic regulatory mapping across ten areas of operations gives rise to the conceptual overlap of all four major frameworks, IMO MSC-FAL.1/Circ.3/Rev.1, the USCG Maritime Cyber Strategy, NIST CSF 2.0, and BIMCO GL4 all remaining conceptually aligned on the same five risk management functions and yet entirely different in operational prescription, offering ship managers no actionable implementation guidance Second, the five-component CSMP framework built via the Layer 2 practitioner analysis introduces the first executable, LNG-specific operational architecture, bridging this gap in prescription in the current ISM Code SMS and adding two new instruments a three-tier LNG asset criticality hierarchy and the Ship-Shore Cyber Interface Register, none of which exist in any existing frameworks. Third, Layer 3 gap analysis reveals that OT/IT convergence is the only area of total regulatory shrinkage across all four tools, and the gap with the highest rating of critical, due to the direct conduit it provides between administrative IT networks and safety-critical safety systems on board the modern LNG boats.

4.1 Regulatory Mapping: Convergence Without Operational Prescription

The regulatory mapping exhibited in Table 1 was obtained through a systematic content analysis of the regulatory and industry guidance documents in ten domains of operational requirements. The examination shows a similar and analytically significant trend: all of the significant regulatory tools have a common high-level conceptualization, the NIST CSF five functions of Identify, Protect, Detect, Respond, and Recover, yet exhibiting a substantial difference in operational specificity by which they transform the functions themselves into practical requirements of ship managers. Circular MSC-

FAL.1/Circ.3/Rev.1 has the most extensive international requirement, but the least operational specificity of all ten domains considered, with a way of defining the requirements expressed in overall principles of requirements leaving all the detail with the ship managers and flag states with no specified final results, performance indicators and minimum standards. The USCG Maritime Cyber Strategy (2021) is more operationally oriented in the way it addresses the requirements of the port interface and the threshold of incident notification, but its technology-focused nature makes it operationally indifferent, at the level of the vessel-type. The most technically granular framework of all domains, NIST CSF 2.0 is not maritime calibrated, so a large amount of specialist interpretive work to convert it into shipboard operational procedures is essential.

The most analytically significant regulation mapping outcome is the overall and comprehensive lack of convergence guidance in OT/IT in all four of the regulatory tools considered. Integrated OT/IT network settings of contemporary LNG carriers, settings where cargo management computers, reliquefication controls and ECDIS, and administrative IT settings are located on network infrastructure are not covered, referenced and even recognized by any of the existing maritime cyber regulatory tools. This is not a lapse of inadequate specificity but a lapse of total regulatory silence: none of four tools discussed give any hint on how operators ought to approach the cyber security consequences of the OT/IT network integration in high-consequence vessels. This result is referred to as Gap 2 in the gap analysis, and it is the most serious regulatory gap found by this research, since a combination of technical severity and extent of consequences, as defined in the literature review, was made.

Table 2:Regulatory Mapping Matrix: Operational Requirements Across IMO, USCG, NIST, and BIMCO Instruments

Requirement Domain	IMO MSC.428(98) / Circ.3 Rev.1	USCG Maritime Cyber Strategy (2021)	NIST CSF 2.0 (Maritime Context)	Operational Gap Identified
Risk Identification & Asset Inventory	Required within SMS per Circ.3 Para 2.1; flag state obligation to ensure identification of critical systems. No minimum asset taxonomy specified.	Requires critical maritime systems inventory for vessels operating in US waters (Strategy Goal 2). No LNG-specific asset categories defined.	ID.AM function: detailed asset management taxonomy required with ownership, communication flows, and external dependencies mapped.	No framework specifies minimum asset classification criteria for LNG cargo systems, ESD networks, or reliquefication plant controls specifically.
Vulnerability Assessment Protocol	Principle-based only; references IEC 62443 without mandating its application. Methodology entirely at ship manager discretion.	Mandates periodic assessments; assessment methodology and frequency at operator discretion.	ID.RA function: structured risk assessment process outlined with threat, vulnerability, and likelihood scoring.	No LNG-specific vulnerability taxonomy exists. OT system assessment methodology not prescribed by any instrument.
Access Control & Authentication	Mentioned in Circ.3 Para 2.3; no minimum standard specified. References but	Specifies need for role-based access in port interface environments; no minimum	PR.AC function: identity management with specific control requirements; PR.PT covers	No minimum access control standard for shipboard OT systems. Third-party terminal access protocols

	does not mandate IEC 62443-2-1.	technical specification.	protective technology.	entirely unaddressed.
Crew Training & Awareness	Subsumed within ISM Code Regulation 6 training obligations; no cyber-specific hours, competency standards, or exercise requirements.	Training mentioned within workforce readiness pillar; no minimum standard, competency framework, or drill requirement specified.	PR.AT function: awareness and training programs required; cybersecurity in supply chain addressed.	No minimum cyber training hours, competency assessment standard, or scenario-based exercise requirements in any instrument.
Incident Detection & Monitoring	Acknowledged in principle; no technical monitoring specification or minimum detection capability defined.	USCG requires notification of reportable cyber incidents; threshold for 'reportable' not defined for cyber events.	DE.AE and DE.CM functions: anomaly detection and continuous monitoring with specific technical controls.	No requirement for OT-specific anomaly detection aboard LNG carriers. Reporting threshold for maritime cyber undefined by USCG.
Incident Response Procedures	Required within SMS emergency procedures (ISM Code Regulation 8); cyber-specific response planning not mandated.	Reportable incidents must be notified by USCG within 24 hours (33 CFR Part 101). Response planning at operator's discretion.	RS.RP, RS.CO, RS.AN functions: detailed response planning, communications, and analysis requirements specified.	Response plans rarely address LNG-specific consequence scenarios including cargo system compromise or ESD bypass events.
Recovery & Business Continuity	Not explicitly addressed in Circ.3 or MSC.428(98) beyond general SMS continuity planning.	Recovery addressed strategically; no operational specifics or minimum recovery time objectives defined.	RC.RP and RC.IM functions: recovery planning and improvements required with specific execution criteria.	No LNG terminal compatibility cyber recovery protocol in any framework. Manual backup procedures for CMS not addressed.
Third-Party & Supply Chain Risk	Not addressed in Circ.3 or MSC.428(98). Shore-side vendor interfaces are not referenced.	Partially addressed for port facility interfaces under MTSA requirements; vessel-terminal digital interfaces not specified.	ID.SC function: supply chain risk management with supplier agreements and assessment programs required.	Most under addressed domain: LNG shore-to-ship data interfaces, charterer monitoring systems, and vendor remote access entirely unregulated.

OT/IT Convergence Management	Not addressed. Network segregation between IT and OT systems not referenced in any IMO cyber instrument.	Not addressed. USCG strategy is technology-neutral and does not distinguish OT from IT environments.	NIST SP 800-82 (OT Guide) addresses convergence in industrial settings but is not incorporated in maritime regulatory context.	MOST CRITICAL GAP: No framework addresses the integrated OT/IT network environments of modern LNG carriers.
SIRE 2.0 / Vetting Alignment	Not referenced. As the higher international authority, IMO does not reference commercial vetting instruments; SIRE 2.0 operates outside the IMO regulatory framework.	Not referenced. The USCG Maritime Cyber Strategy is a federal regulatory instrument and does not engage with OCIMF commercial vetting mechanisms.	Not referenced. NIST CSF is a technical risk management framework with no scope over commercial vetting regimes.	SIRE 2.0 Q.7.1 series requires CSMP documentation and cyber governance evidence; no standard CSMP format or minimum content is specified.

Note. IMO = International Maritime Organization; USCG = United States Coast Guard; NIST CSF = NIST Cybersecurity Framework 2.0 (2024); BIMCO GL4 = BIMCO Cyber Security Guidelines, 4th Edition (2021).

In table 2, operational gap assessment derived from practitioner Layer 2 analysis cross-referenced with SIRE 2.0 Q.7.1 question framework (OCIMF, 2023). All four frameworks assessed in most current published versions as of December 2024. The five-component CSMP framework presented above represents a substantive operational advance beyond all currently available regulatory and industry instruments. Where IMO Circular MSC-FAL.1/Circ.3/Rev.1 articulates cyber risk management obligations in principle without prescribing minimum standards, the CSMP framework provides explicit, executable specifications for each operational domain, including minimum training hours, bi-annual assessment cycles, tiered classification criteria, and a four-level incident classification system with defined USCG notification thresholds. Where the BIMCO Cyber Security Guidelines (4th Edition, 2021) explicitly exclude vessel-type-specific guidance from their scope, the CSMP framework is calibrated specifically for LNG carrier and tanker OT architectures, including LNG-consequence scenarios in vulnerability assessments and explicitly addressing the ESD and CMS systems that constitute the highest-consequence attack surface in gas carrier operations. Where SIRE 2.0 requires CSMP documentation without specifying minimum content, the framework provides the complete operational architecture that SIRE 2.0 assesses but does not define. The Ship-Shore Cyber Interface Register introduced in Component 5 addresses a category of risk, vessel-terminal digital interface management during LNG loading operations, that is entirely absent from all four instruments examined, representing the framework's most operationally novel contribution.

4.2 The Five-Component CSMP Framework

Table 2 shows the five component CSMP framework that was developed as a result of the Step 2 practitioner analysis. The framework is to be integrated with the current ISM Code Safety Management System architecture, i.e., in the context of the current existing procedures to operational safety, emergency preparedness, and document control in the existing SMS as opposed to a complementary management system. This design principle is also based on the guidance of the resilience engineering framework that adaptive capacity is best developed through current organizational structures and the

practical aspect of operation that LNG and tanker ship managers are already under the strict operation SMS documentation mandates; a framework that competes with current management operations by establishing parallel administrative structures would hamper instead of help improve operational cyber resilience.

Many of the components in the hierarchy are component 1 (Asset Classification and Criticality Ranking), which introduces a three-tier hierarchy of criticality highly optimized to LNG carrier and tanker system designs. The tiering of LNG, specifically designating ESD systems, gas detection networks, and reliquefication plant controls as Tier 1 Safety-Critical assets, is also not found in any of the current regulatory tools and industry standards, which approach vessel assets in a non-differentiated manner regardless of cargo type or severity of consequences. This tiering has an implication of security controls: Tier 1 assets must have the most stringent security controls, OT-network credential systems, and must be included in the threat and vulnerability assessment protocol defined in Component 2.

Component 5 (Recovery, Continuity, and Third-Party Interface Management) presents the Ship-Shore Cyber Interface Register which is a totally new operational tool that was created during the analysis of operations performed by practitioners in the field of LNG carrier operations in terminals such as Cameron LNG and through the identification of the fact that LNG terminal operations include multiple simultaneous digital interconnections that cannot be managed by an existing tool. A modern LNG carrier which is engaged in loading operations at a US export terminal has four to seven concurrent external digital connections regularly: terminal loading arm control system interface, charterer cargo monitoring feed, classification society remote survey connection, ship manager monitoring system, pilot communication system, and in certain instances USCG inspection data transmission. Any existing maritime cyber security instrument does not tackle any of these interfaces. All such interfaces are given operational governance mechanism by the Register, which is consistent with the focus of the USCG Strategy on the partnership-based maritime security and offers operational specificity not offered by the strategy itself.

Table 3:Five-Component CSMP Framework for LNG and Tanker Fleet Operations

Component	Description	Operational Specification	Regulatory Alignment	Gap Addressed
Component 1, Asset Classification & Criticality Ranking	Systematic identification and risk-tiered classification of all IT and OT systems aboard LNG/tanker vessels into three criticality tiers: (1) Safety-Critical, (2) Operationally Critical, and (3) Administratively Important. Tier assignment governs the security control level applied to each system.	Tier 1 [Safety-Critical]: Cargo Management System (CMS), ECDIS, Emergency Shutdown (ESD) system, Gas Detection System, Emergency Communication. Tier 2 [Operationally Critical]: Reliquefication plant controls, Ballast Management System, Engine Room Monitoring. Tier 3 [Administrative]: Crew welfare IT, email, administrative servers. Network segregation enforced	IMO Circ.3 Para 2.1; NIST CSF 2.0 ID.AM; SIRE 2.0 Q.7.1.1; BIMCO GL4 Chapter 3	Closes the asset inventory gap. Provides foundational baseline without which all subsequent components are inexecutable. LNG-specific tiring of ESD and CMS is novel and absent from all existing frameworks.

		between Tier 1 and Tier 3.		
Component 2, Threat & Vulnerability Assessment Protocol	Structured bi-annual OT/IT vulnerability assessment using a four-step protocol: (1) system boundary mapping by tier, (2) threat actor profiling, (3) attack vector analysis per system, (4) consequence severity rating calibrated for LNG cargo operations. Findings documented in a Vessel Cyber Risk Register updated biannually and reviewed after significant system changes.	Mandatory assessment scope: ECDIS firmware and chart data integrity; CMS shore interface connections; satellite communication systems; all vendor remote access sessions; reliquefication plant control network. Consequence severity rating must include LNG-specific outcomes: cargo quantity manipulation, ESD bypass, gas detection alarm suppression. Assessment outcomes formally reviewed by DPA.	IMO Circ.3 Para 2.2; NIST ID.RA; USCG Strategy Goal 2; IEC 62443-3-2 (risk assessment); SIRE 2.0 Q.7.1.2	Provides a vessel-type-specific methodology absent from all regulatory instruments. Explicitly requires LNG consequence scenarios in assessment scope, directly addressing the OT/IT convergence gap (Gap 2) at the assessment level.
Component 3, Access Control & Crew Awareness Standards	Role-based access control matrix for all shipboard systems, differentiated by tier. Combined with mandatory minimum 8-hour annual cyber awareness training for all officers, supplemented by LNG-scenario tabletop exercises for senior officers (Master, Chief Officer, Chief Engineer) conducted minimum annually.	Tier 1 systems: dedicated OT-network credentials segregated from IT credentials; no shared passwords; two-factor authentication for all remote access by shore-based personnel. Crew training program: annual 8-hour online + shipboard module for all officers; annual 4-hour awareness for ratings. Tabletop exercise scenarios specific to LNG operations: simulated CMS manipulation during loading, ECDIS data corruption during pilotage, phishing compromise of shore monitoring access.	IMO Circ.3 Para 2.3; NIST PR.AC, PR.AT; SIRE 2.0 Q.7.1.3, Q.7.1.4; BIMCO GL4 Chapters 5 and 6; ISM Code Regulation 6	Directly addresses crew awareness gap (Gap 1) and access control deficiency. Tabletop exercise requirement specifically targets incident reporting culture gap (Gap 4). LNG-specific scenarios are entirely novel; no existing framework specifies vessel-type training content.
Component 4, Incident	Stepped detection architecture	Detection: OT anomaly monitoring	IMO Circ.3 Para 2.4; USCG 33	Closes incident detection and

Detection, Response & USCG-Aligned Reporting Chain	combining network traffic monitoring, OT-specific anomaly alerts, and a four-level incident classification matrix with defined escalation thresholds and USCG notification alignment. Incident response procedures embedded within existing SMS emergency response architecture.	alerts for Tier 1 systems; network traffic baseline deviation alerts for Tier 2. Classification: Level 1 [Crew self-resolution, logged internally]; Level 2 [Shore DPA notification within 4 hours]; Level 3 [USCG notification within 24 hours per 33 CFR Part 101, Serious Marine Incident threshold]; Level 4 [Incident Management Centre activation, full emergency response]. Response procedures include LNG cargo operations suspension criteria for Levels 3–4.	CFR Part 101; NIST DE.AE, RS.RP, RS.CO, RS.AN; SIRE 2.0 Q.7.1.5; OCIMF TMSA 3 KPI 9A	reporting gaps (Gaps 4 and 5). Provides USCG-aligned notification thresholds currently absent from operational CSMPs. Level 1-2 internal capture mechanism specifically designed to cultivate reporting culture without triggering regulatory notification for near misses.
Component 5, Recovery, Continuity & Third-Party Interface Management	Documented cyber recovery procedures for each Tier 1 system, including manual backup operating procedures for cargo and navigation. Combined with a novel formal instrument, the Ship-Shore Cyber Interface Register, governing all digital connections between the vessel and external parties.	Recovery: manual backup procedures for CMS, ECDIS, and ESD systems documented and drilled annually; recovery time objectives defined per system. Ship-Shore Cyber Interface Register: formal inventory of all external digital interfaces (LNG terminal loading arm control systems; charterer cargo monitoring feeds; classification society remote survey; ship manager monitoring; vendor remote access). Each interface entry includes interface type, data exchanged, access credentials governance, cyber	NIST RC.RP, RC.IM; USCG Strategy Goal 3; SIRE 2.0 Q.7.1.6; BIMCO GL4 Chapter 7; OCIMF TMSA 3 KPI 9A; IEC 62443-2-4	Closes recovery and third-party interface gaps (Gaps 3 and 5). The Ship-Shore Cyber Interface Register is an entirely novel operational instrument absent from all existing frameworks. Directly addresses the US LNG export terminal interface context, operators at Cameron LNG, Sabine Pass, and Freeport LNG typically manage 4–7 simultaneous external digital connections during loading operations.

		risk rating, and formal access agreement reference—entire Register reviewed against SIRE 2.0 Q.7.1.6 criteria.		

Note. CSMP = Cyber Security Management Plan; ESD = Emergency Shutdown System; CMS = Cargo Management System; ECDIS = Electronic Chart Display and Information System; OT = Operational Technology; IT = Information Technology; DPA = Designated Person Ashore; ISM = International Safety Management Code; BIMCO GL4 = BIMCO Cyber Security Guidelines 4th Edition; OCIMF TMSA 3 = Tanker Management Self-Assessment 3rd Edition; IEC 62443 = Industrial Automation and Control Systems Security standard series.

The CSMP framework goes beyond the entire arsenal of instruments at present in three different ways. First, where IMO Circular MSC-FAL.1/Circ.3/Rev.1 outlines what cyber risk management should accomplish without defining how the operational standards should be minimum, the CSMP outlines practical requirements of all domains such as number of training hours needed, frequency of assessment, access levels, and four tiers of incident threshold with prescribed USCG notification conformity. Second, when BIMCO GL4 expressly lacks coverage of vessel-type guidance, the CSMP specifically supports LNG carrier and tanker OT designs, with LNG-consequence scenarios (ESD bypass, CMS manipulation, gas detection suppression) which any general framework does not cater to. Third, the Ship-Shore Cyber Interface Register presented in Component 5 regulates vessel-terminal digital connections in the process of LNG loading operations - a type of risk not addressed in IMO, USCG, NIST, BIMCO, and SIRE 2.0 documents. The operational specification level needed by ship managers to implement directly is seen as a combination of five implementation gaps that are recognized in this paper, all of which no existing framework covers at the same time.

4.3 Operational Gap Analysis

The Step 3 gap analysis delivered five discrete implementation gaps between regulatory requirements and operational practice in LNG and tanker fleet cyber security management. The regulatory gaps are not evenly distributed throughout the regulatory environment: they are concentrated at the border between the regulatory principle and operational delivery, which affirms the theoretical hypothesis, based on the resilience engineering model, that the maritime cyber security predicament is intrinsically an issue of implementation structure, but not regulatory aspirations. In Table 3, the gaps analysis is obtained.

Gap 2 (OT/IT Convergence) is determined to be the most serious in terms of severity and consequence aspects. Its critical rating indicates three compounding factors: (a) it portrays a real technical vulnerability within a physical network topology of modern LNG carriers that cannot be remedied by any head of procedure or documentary solutions; (b) it is not addressed at all by all four regulatory instruments analyzed and is completely missing in even the SIRE 2.0 questionnaire paradigm; and (c) its hypothetical impact in the LNG operational context, cyber-induced ESD system compromise in the process of cargo operations in a large terminal is disastrous in terms of both safety and Gap 5 (LNG-Specific USCG Guidance) is also rated high in consequence but medium in operator-level implementation difficulty due to the analytically importance difference between operator-addressable and policy-addressable gaps: ship managers can implement the Ship-Shore Cyber Interface Register (Component 5) to provide federal policy-relevant compensating control to the vessel level, but the underlying USCG and FERC regulatory gap cannot be addressed at the operator level of implementation.

Table 4:Operational Gap Analysis Matrix: LNG and Tanker Fleet Cyber Security Implementation

Gap	Description	Severity & Consequence	Current Regulatory Treatment	CSMP Framework Response	Implementation Difficulty
Gap 1 Crew Cyber Awareness	Significant discrepancy between regulatory training expectations and actual crew cyber competency levels, particularly among officers transitioning from older fleets with limited digital integration and among non-officer ratings with unrestricted device use aboard vessels.	High. Affects all vessel types. Directly linked to phishing susceptibility, unauthorized device connection, and password sharing, the most common initial attack vectors documented in maritime cyber incidents (DNV, 2023).	None of the major frameworks specify minimum training hours, competency assessment methodology, or scenario-based exercise requirements. ISM Code Reg. 6 training obligations apply generically.	Component 3: Mandatory 8-hour annual training; LNG-specific tabletop exercises; competency logging in SMS training records.	Medium. Achievable within current ISM training framework given owner investment. Primary barrier is operational scheduling, not technical complexity.
Gap 2 OT/IT Convergence (CRITICAL)	Modern LNG carriers operate deeply integrated OT/IT network environments in which CMS, reliquefication plant controls, ECDIS, and administrative systems share common network infrastructure, creating lateral movement pathways from low-security IT to safety-critical OT systems. No regulatory instrument addresses this architecture.	Critical. An IT-Step compromise on a modern LNG carrier can provide cyber-pathway access to the Tier 1 ESD system within 3–4 lateral network hops (Mitropoulos & Xenakis, 2022). Consequence severity: catastrophic, potential for cyber-induced uncontrolled LNG release indistinguishable from physical attack (Marroni et al., 2023)	Not addressed by IMO Circ. 3, USCG Strategy, NIST CSF in maritime OT application, or BIMCO GL4. IEC 62443 referenced but not mandated. SIRE 2.0 Q.7.1 does not assess network architecture.	Components 1 + 2: Tier classification enforces OT/IT boundary definition; Component 4: OT-specific anomaly detection as compensating control while hardware segregation is implemented.	High. Requires hardware network segregation investment. Technical complexity and cost are significant for existing fleet; new-built design integration is more feasible.
Gap 3 Third-Party & Port Interface Risk	LNG terminal data interfaces, charterer vessel monitoring systems, vendor remote access connections, and cargo measurement system data transfers represent uncontrolled cyber	High. Particularly acute for LNG vessels at US export terminals where multiple third-party data systems interface with shipboard CMS and navigation	Only NIST ID.SC partially addresses supply chain risk; not applied to maritime ship-shore interfaces. MTSA regulations	Component 5: Ship-Shore Cyber Interface Register; formal third-party cyber risk assessment protocol embedded in SMS.	Medium-High. Procedural controls (Register) achievable by operators. Technical interface controls require cooperation and standardization across terminal operators, beyond unilateral operator capability.

	entry points into shipboard systems. No current framework addresses vessel-terminal digital interface management.	systems simultaneously during loading operations. Charterer cargo monitoring feeds introduce continuous external data connections throughout voyages.	address port facility physical security; digital interface security is not addressed.		
Gap 4 Incident Reporting Culture	Documented organizational reluctance among tanker and LNG fleet operators to formally report cyber incidents and near-misses due to fears of vetting consequences, SIRE 2.0 inspection exposure, and operator scrutiny. Results in structural under-reporting that breaks industry-level risk feedback loops.	Medium-High. Without accurate incident data, the collective maritime cyber risk picture remains fundamentally incomplete. Regulatory improvement feedback loops are broken. (DNV, 2023). estimates documented incidents represent fewer than 40% of actual events.	USCG 33 CFR Part 101 requires notification for serious incidents, but threshold is undefined for cyber events. No near-miss reporting framework exists for maritime cyber at any level. SIRE 2.0 cyber questions create commercial disincentive against voluntary disclosure.	Components 3 + 4: Reporting culture addressed through tabletop exercises; Levels 1–2 of incident classification specifically designed for internal near-miss capture below USCG notification threshold.	High. Fundamental cultural change challenge requiring explicit top-management commitment, no-blame near-miss reporting policy, and confirmation that Level 1–2 reporting will not trigger commercial consequences.
Gap 5 LNG-Specific USCG Cyber Guidance	The USCG Maritime Cyber Strategy and associated port security regulations apply to all vessels and port facilities generically. No LNG-specific cyber guidance addresses the unique vulnerabilities of cryogenic cargo systems, ESD interfaces, or the digital connectivity requirements of US LNG export terminal operations.	High. US LNG export terminals including Cameron LNG, Sabine Pass LNG, Freeport LNG, and Corpus Christi LNG constitute critical national energy and foreign policy infrastructure. Cyber incidents at these terminals carry national security implications extending beyond the immediate maritime safety event.	USCG strategy is intentionally technology-neutral. MTSA regulations predate modern LNG cyber vulnerabilities—no LNG-specific guidance from USCG, FERC, or DOE. IMO has not issued vessel-type-specific cyber guidance for any ship type.	Components 4 + 5: USCG-aligned notification thresholds embedded in incident classification; Ship-Shore Register directly manages US LNG terminal interface exposure at operator level.	Medium from operator perspective. Regulatory gap at USCG/FERC level is not addressable by ship operators alone; gap closure requires federal policy action targeting LNG-specific maritime cyber standards.

Note. Severity ratings (Critical, High, Medium) reflect the combination of likelihood of gap manifestation in operational environments and consequence magnitude specific to LNG and tanker fleet operations. Implementation difficulty ratings reflect operator-level feasibility given current industry resources, technology availability, and the regulatory environment. All severity ratings derived from practitioner analysis cross-referenced with published survey data (DNV, 2023); Hopcraft et al. (2023); *BIMCO/Thetius, 2022).*

The gap analysis presented in Table 4 yields three findings of particular analytical significance. Gap 2 (OT/IT Convergence) is the only gap rated Critical, reflecting its unique combination of technical severity, complete regulatory invisibility, and catastrophic consequence potential in the LNG operational context. It is also the gap most resistant to procedural remediation alone: unlike Gaps 1 and 4, which can be substantially closed through training programs and reporting policy changes, Gap 2 requires hardware network segregation investment that goes beyond documentation and procedure. Gap 5 (LNG-Specific USCG Guidance) is the only gap whose closure lies substantially outside operator authority, it requires federal policy action by the USCG, FERC, or DOE, yet its consequence rating is High because US LNG export terminal operations of national strategic significance remain entirely unprotected by vessel-type-specific regulatory guidance.

The implementation difficulty ratings reveal a practically important pattern: the three gaps most amenable to operator-level resolution (Gaps 1, 3, and 4) have Medium to Medium-High difficulty ratings, indicating that they are achievable within current industry resource constraints given management commitment, and that the primary barriers are cultural and organizational rather than technical or financial. Similar resistance to integrating new systems within established professional environments has been observed across sectors, particularly where workflow disruption and ethical or operational concerns are anticipated (Abu-Farha et al., 2026).

Compared to existing frameworks, the CSMP proposed in this study is the only instrument that simultaneously identifies, quantifies, and provides operational responses to all five gaps. The BIMCO Guidelines address aspects of Gaps 1 and 3 but provide no LNG-specific guidance and no gap severity rating methodology. The MaCRA framework addresses Gap 2 technically but provides no organizational architecture for SMS integration. No existing regulatory instrument addresses any of the five gaps at the operational specification level that ship managers require for implementation.

Discussion

The findings of this research identify three analytically meaningful results that contribute to the knowledge about the implementation of maritime cyber security in the LNG and tanker industry and interact with the literature in the field significantly. To begin with, the regulatory mapping validates and deepens the results of Progoulakis et al. (2021) and Afenyo and Caesar (2023) confirming that the gap does exist between maritime cyber regulation and operational practice, but also suggesting that this gap has a definite structure: it is most extensive and most influential at the vessel-type level and at the OT/IT interface, which any scholarly research and regulatory tools lack the most substantive operational coverage. The most detailed published alignment of IMO, USCG, NIST and BIMCO requirements with individual operational domains currently in existence, the ten-domain regulatory mapping matrix (Table 1) is expanding the currently existing literature considerably, with its core conclusion being full regulatory silence on OT / IT convergence across all four charts. The vulnerability of OT/IT convergence into maritime scenarios, as set by Bolbot et al. (2022) and Enoch et al. (2021), is demonstrated in the technical literature but goes unnoticed by the regulatory environment as the final result of the present work, which will directly translate into the regulation reform agenda.

Moreover, the practitioner-driven CSMP framework (Table 2) goes further than the current contributions as it does not present a theoretical view as to what cyber security management should be like but a practically applicable architecture that can be enacted under the current SMS. This is unlike the MaCRA model developed by Tam and Jones (2019) which presents a complex risk assessment methodology but fails to offer an organization-level architectural framework through which the findings of assessment can be translated into operational practices and the frameworks generated by the edited volume by Kechagias et al. (2022) which present sophisticated theoretical and case study

work without a practical implementation framework. The introduction of the Ship-Shore Cyber Interface Register, which is a component of Component 5, is, as far as the author can determine, a completely new operational tool in the literature of cyber security in the maritime sector, which derives directly out of the practitioner experience of what it is like to operate LNG carriers at terminals such as Cameron LNG and out of recognition of the fact that there is no extant tool which governs the variety of multiple digital interfaces present during LNG terminal operations. This is a process that will fill a regulatory gap that the literature has failed to recognize not to mention the fact that it has not been addressed (Bolbot et al., 2022; Melnyk et al., 2025).

Furthermore, the findings of the gap analysis have implications which spans more than maritime cyber security to the overall question of how high-consequence industries ought to organize the interaction between regulatory compliance and operational resilience. The incident reporting culture gap (Gap 4) is especially didactic in that respect. Hopcraft et al. (2023) reported the under-reporting in the field of maritime cyber security with references to the organizational cultures of vetting exposure avoidance over the collective risk minimization. The gap in the present study framework response, the design of a four-level incident classification system, internal-capture levels set at below the USCG notification threshold, is within the prescriptive Weick and Sutcliffe (2001) of the HRO literature that organizations that maintain authentic operational reliability need to develop reporting systems commensurate to the severity of events, that is, explicitly distinguishing between learning-oriented near-miss capture and regulatory notification. It is a theoretically based extension of current compliance model that SIRE 2.0 and IMO auditing currently reward, and it sets the direction towards a more basic redefinition of the way maritime industry responds to cyber incident information to enhance its overall resilience (Grbić et al., 2018; Pavić et al., 2024).

The findings of this study carry direct and concrete implications for three groups of stakeholders engaged with US maritime cyber security. For LNG fleet operators, the regulatory mapping confirms that current SIRE 2.0 and IMO audit compliance does not constitute cyber resilience, it constitutes documentation of intent. The CSMP framework provides the operational architecture through which that intent becomes practice, particularly through Component 4's four-level incident classification system, which enables operators to build genuine reporting culture without triggering commercial consequences for near-miss disclosure. For USCG and US federal regulators, the study's finding that no LNG-specific maritime cyber guidance exists from any US regulatory authority, despite Cameron LNG, Sabine Pass, Freeport LNG, and Corpus Christi LNG collectively constituting critical national energy infrastructure, represents an actionable policy gap of national security significance. The CSMP framework's Component 4 notification thresholds and Component 5 Ship-Shore Cyber Interface Register provide practitioner-developed models that USCG could adopt directly as the basis for LNG-specific cyber guidance without requiring new primary research. For the international maritime community, the ten-domain regulatory mapping matrix provides the most comprehensive published alignment of IMO, USCG, NIST, and BIMCO requirements currently available, establishing an evidence base that flag states, classification societies, and OCIMF could use to develop the prescriptive minimum standards that all four instruments currently lack.

The strategic interest of the United States in the cybersecurity of LNG carriers extends well beyond maritime safety: US LNG exports to European and Asian allies constitute a core instrument of American energy diplomacy (Bolbot et al., 2022). Cameron LNG, Sabine Pass, and Freeport LNG have a combined effect of ensuring energy diversification strategies in the European and Asian countries, and disruption of the US LNG export activities as a result of a cyber incident would have both the geopolitical and economic implications. This strategic context should be interpreted as the US federal maritime and energy regulatory agencies priority in terms of the gap analysis finding that no LNG-specific USCG or FERC cyber guidance is available (Gap 5) (Marroni et al., 2023; Shawon et al., 2024). The CSMP model proposed in this paper, especially the Ship -Shore Cyber Interface Register and the USCG-oriented incident notification threshold built into Component 4, a practitioner-developed model has the potential to inform the development of LNG-specific USCG guidance, to be developed before the current regulatory vacuum and the actual creation of a formal instrument.

Limitations

Three limitations warrant acknowledgement. First, the Layer 2 framework construction draws on practitioner experience and operational environment; while designed for sector-wide applicability, systematic adaptation would be required for other vessel types, flag states, or operator scales. Second, the qualitative methodology does not permit statistical generalization of the gap analysis findings; the five gaps are analytically derived and practitioner-validated rather than statistically established across a representative operator sample. Third, the regulatory landscape reflects instruments current as of December 2024 and will require revision as IMO, USCG, or NIST guidance evolves. Regarding potential confirmation bias from the author's direct industry involvement: this was mitigated through regulatory triangulation across four independent instruments, cross-referencing of all gap severity ratings against published survey data (DNV, 2023; Hopcraft et al., 2023), and benchmarking of all framework components against SIRE 2.0 criteria as an externally developed standard. These measures materially reduce, though do not eliminate, the bias inherent in practitioner-led research.

Conclusion

This study has established three principal findings. First, current international and US maritime cyber security regulatory frameworks, while convergent in conceptual architecture, are structurally insufficient to deliver the operational prescriptiveness required by LNG and tanker ship managers, producing a compliance-execution void that no existing instrument closes. Second, the gap between regulatory compliance and operational resilience is widest and most consequential at the OT/IT convergence interface and the LNG terminal-vessel digital boundary, precisely the two domains of complete regulatory silence across all four frameworks examined. Third, the five-component CSMP framework developed through this study's three-layer practitioner analysis, including the novel Ship-Shore Cyber Interface Register, demonstrates that operationally specific, vessel-type-calibrated cyber resilience frameworks are both achievable within existing SMS structures and immediately deployable without awaiting regulatory mandate. The study's theoretical contribution lies in demonstrating that resilience engineering and HRO theory expose a structural incompatibility between compliance-oriented maritime cyber regulation and the adaptive capacity requirements of high-consequence LNG operations. Its policy contribution lies in providing the first systematic evidence base for LNG-specific USCG maritime cyber guidance, a regulatory development that US national energy security urgently requires given the strategic significance of Cameron LNG, Sabine Pass, and Freeport LNG to American energy diplomacy. Future research should prioritize longitudinal empirical validation of the CSMP framework across diverse fleet contexts, controlled OT penetration testing of LNG carrier network architectures, and cross-domain extension of the framework to port infrastructure and offshore platform environments. Specific, vessel-type-calibrated cyber resiliency frameworks of LNG carriers have become the subject of regulation compliance rather than national critical infrastructure protection.

Practical Implications

The CSMP framework provides an immediately actionable pathway for three audiences. For LNG fleet operators and ship managers, implementation follows the framework's component sequence within the existing SMS, from Component 1 asset classification (two to three weeks, desk-based) through Component 5 Ship-Shore Cyber Interface Register (reviewed at each terminal call), requiring approximately 80–120 person-hours of management effort and one 8-hour annual crew training module per officer, with hardware network segregation best incorporated into planned dry-dock cycles. For USCG and US regulators, the regulatory mapping matrix, four-level incident classification system, and Ship-Shore Register provide three ready-to-adopt policy instruments for LNG-specific cyber guidance development under 33 CFR Part 101, without requiring new primary research. For OCIMF and the oil major vetting community, the CSMP component specifications in Table 2 supply the minimum content standard that SIRE 2.0 Q.7.1 currently demands but does not define, enabling an industry-wide compliance baseline in place of the inconsistent operator responses presently generated by vetting cyber questions.

Future Research Directions

Four research directions merit priority based on the results of the study. First, longitudinal fleet-scale studies are needed to empirically validate the CSMP framework across diverse operator contexts and to develop quantitative cyber resilience KPIs measuring the compliance–resilience gap over time. Second, controlled OT penetration testing on LNG carrier network architectures would empirically map lateral attack paths, providing the technical evidence base for Gap 2's hardware segregation recommendations that the present study identifies but cannot resolve through qualitative methods alone. Third, AI-based anomaly detection applied to LNG carrier OT network traffic represents a natural extension of the Component 1 three-tier asset criticality hierarchy; future research should investigate whether the CSMP tier classifications can serve as training data schemas for vessel-specific real-time threat identification models. Fourth, the Ship-Shore Cyber Interface Register and gap analysis methodology are directly transferable to port infrastructure, offshore platforms, and FSRU environments, all facing analogous vessel-terminal digital interface challenges, and cross-domain extension would substantially amplify the framework's academic and policy contribution beyond the LNG and tanker sector..

References

Aboshighiba, H., Benariba, A., Sbaa, M. R., Souad, M., Sidamar, L., Suleiman, R. K., ... & Meliani, M. H. (2025). Modeling of Textured Hydrostatic Thrust Bearings and Lubricating Films with Variable Thickness. Arabian Journal for Science and Engineering, 50(4), 2911-2923. https://doi.org/10.1007/s13369-024-09645-8

Abualhomos, M., Shihadeh, A., A Abubaker, A., Al-Husban, K., Fujita, T., Alsaraireh, A. A., ... & Al-Husban, A. (2025). Unified framework for type-n extensions of fuzzy, neutrosophic, and plithogenic offsets: Definitions and interconnections. Journal of fuzzy extension and applications, 6(4), 689-726. https://doi.org/10.22105/jfea.2025.514314.1858

Abu-Farha, R. K., Alzoubi, K. H., Al Safadi, A. A., Alsous, M. M., Nawasreh, A., El-zubi, M. K., & Al-Ashwal, F. Y. (2026). Exploring Physicians' Willingness to Integrate Artificial Intelligence in Clinical Practice: Ethical and Practical Insights From a Jordanian Cross-Sectional Survey. Health Science Reports, 9(3), e71994. https://doi.org/10.1002/hsr2.71994

Adaileh, A., Abu-Rayyan, A., Khasawneh, A., & Alahmad, W. (2025). A comparative study of GO/TiO2/SiO2 catalysts for the photocatalytic degradation of methylene blue and phenolic compounds. Environmental Quality Management, 34(3), e70058. https://doi.org/10.1002/tqem.70058

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, 106493.

Alkasasbeh, A. M., Jarrah, S. S., Alhusamiah, B. K., & Tarawneh, F. S. (2025). Factors influencing the utilization and adoption of electronic health records among nurses in Jordanian hospitals. Jordan Journal of Nursing Research, 4(1), 68-80. https://doi.org/10.14525/JJNR.v4i1.08

Androjna, A., Perkovič, M., Pavic, I., & Mišković, J. (2021). AIS Data Vulnerability Indicated by a Spoofing Case-Study. Applied Sciences, 11(11), 5015. https://doi.org/10.3390/app11115015

Bekiashev, K. A., & Serebriakov, V. V. (1981). Oil Companies International Marine Forum (OCIMF). In International Marine Organizations (pp. 207-216): Springer Netherlands.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. International Journal of Critical Infrastructure Protection, 39, 100571. https://doi.org/https://doi.org/10.1016/j.ijcip.2022.100571

Bolbot, V., Theotokatos, G., Bujorianu, L. M., Boulougouris, E., & Vassalos, D. (2019). Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. Reliability Engineering & System Safety, 182, 179-193. https://doi.org/10.1016/j.ress.2018.09.004

Dimakopoulou, A., & Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2. 0. Journal of Marine Science and Engineering, 12(6), 919.

DNV. (2023). Maritime Cyber Priority 2023: Staying secure in an era of connectivity (DNV, Issue. https://www.dnv.com/cyber/insights/publications/maritime-cyber-priority-2023/

Enoch, S. Y., Lee, J. S., & Kim, D. S. (2021). Novel security models, metrics and security assessment for maritime vessel networks. Computer Networks, 189, 107934.

Grbić, L., Čulin, J., & Perković, T. (2018). SIRE inspections on Oil tankers. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 12(2).

Hollnagel, E. (2017). Safety-II in Practice. In: Routledge.

Hopcraft, R., Tam, K., Misas, J. D. P., Moara-Nkwe, K., & Jones, K. (2023). Developing a maritime cyber safety culture: Improving safety of operations. Maritime Technology and Research, 5(1), 258750-258750.

Kalogeras, G. (2023). Navigating the waters of maritime cybersecurity with BIMCO's guidelines: identifying vulnerabilities and mitigating threats to IT and OT systems Πανεπιστήμιο Πειραιώς].

Kayişoğlu, G., Yilmaz Bolat, P., & Tam, K. (2022). Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships.

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526.

Kim, J., & Lee, S. Y. (2025). Cyber Resilience of Ships: An Evaluation of Guideline and Frameworks. IEEE Access.

Longo, G., Lupia, F., Pugliese, A., & Russo, E. (2024). Physics-aware targeted attacks against maritime industrial control systems. Journal of Information Security and Applications, 82, 103724.

Marroni, G., Moreno, V. C., Ovidi, F., Chiavistelli, T., & Landucci, G. (2023). A methodology for risk assessment of LNG carriers accessing vulnerable port areas. Ocean Engineering, 273, 114019.

Mäurer, N., Guggemos, T., Ewert, T., Gräupl, T., Schmitt, C., & Grundner-Culemann, S. (2022). Security in Digital Aeronautical Communications A Comprehensive Gap Analysis. International Journal of Critical Infrastructure Protection, 38, 100549. https://doi.org/10.1016/j.ijcip.2022.100549

Melnyk, O., Drozdov, O., & Kuznichenko, S. (2025). Cybersecurity in maritime transport: An international perspective on regulatory frameworks and countermeasures. Lex Portus, 11, 7.

Oluwoye, J., & Oyedeji Oluwoye, M. S. (2020). Cybersecurity Issues in Modern Transportation Infrastructure Age: Development of Prototype Maritime and Cargo Security Supply Chain. IAR Journal of Engineering and Technology, 01(02), 1-6. https://doi.org/10.47310/iarjet.2020.v01i02.005

Pavić, V., Barić, M., Grbić, L., & Mišlov, I. (2024). SIRE 2.0–Integration of Human Factors into the Tanker Inspection Program. Theory and Practice of Shipbuilding: Proceedings of the 26th Symposium (SORTA 2024), Zadar, Croatia, 2-5 October 2024,

Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.

Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357-372.

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering, 9(12), 1384. https://doi.org/10.3390/jmse9121384

Putra, I. N., Octavian, A., Heikhmakhtiar, A., Tjahjadi, H., & Susilo, A. K. (2023). Cyber threat analysis of maritime cybersecurity using AHP-topsis. Journal of Maritime Research, 20(2), 13-24.

Patyrykin, K., & Vasyukova, L. (2025). Environmental Accountability or Symbolic Compliance? A Critical Review of ESG Ratings, Greenwashing, and Indirect Emissions in the Global Insurance Sector. International Journal of Energy Economics and Policy, 15(6), 917-925.

Putra, I. N., Octavian, A., Susilo, A. K., & Santosa, Y. (2024). An assessment of cyber resilience in the maritime domain using system dynamics and analytical hierarchy process (AHP). Transactions on Maritime Science, 13(2).

S. Gopinath, M. Hemanand, P. Arunprasath, M. Vivek, P. Balaji, & Charan, S. S. L. (2025). Maritime Cyber security. International Research Journal on Advanced Engineering and Management (IRJAEM), 3(02), 167-172. https://doi.org/10.47392/irjaem.2025.0029

Sarfaraz, T. (2025). Evaluating the Effectiveness of Zero Trust Architecture in Modern Enterprises. Moderating Role of Organisational Maturity. AJBMSS-Advance Journal of Business Management and Social Sciences, 1(2). https://doi.org/10.65080/dp4w1990

Shawon, R. E. R., Dalim, H. M., Shil, S. K., Gurung, N., Hasanuzzaman, M., Hossain, S., & Rahman, T. (2024).

Assessing geopolitical risks and their economic impact on the USA using data analytics. Journal of Economics, Finance and Accounting Studies, 6(6), 05-16.

Svilicic, B., Rudan, I., Jugović, A., & Zec, D. (2019). A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering, 7(10), 364. https://doi.org/10.3390/jmse7100364

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs, 18(1), 129-163. https://doi.org/10.1007/s13437-019-00162-2

Tsailas, D. N. (2025). Risks And Threats In The 21st Century Maritime Security. Security Science Journal, 6(1), 106-144.

USCG CYBER STRATEGIC OUTLOOK. (2021). https://events.iala.int/content/uploads/2021/09/2021-Cyber-Strategic-Outlook.pdf

Weick, K. E., & Sutcliffe, K. M. (2001). Managing the unexpected (Vol. 9). San Francisco: Jossey-Bass.

.