INSTITUTE FOR
HOMELAND SECURITY

Comprehensive Cybersecurity Risk Assessments for Maritime Transportation Systems

Institute for Homeland Security

Sam Houston State University

Cihan Varol, Ph.D

Sam Houston
State University

Comprehensive Cybersecurity Risk Assessments for Maritime Transportation Systems

Cihan Varol
Department of Computer Science
Sam Houston State University
cvarol@shsu.edu

Executive Overview

Maritime transportation systems underpin global trade, national security, and economic stability, carrying approximately 80 percent of worldwide cargo by volume. Over the past two decades, the maritime sector has undergone rapid digital transformation driven by the adoption of interconnected navigation, communication, and logistics technologies. Modern vessels and ports increasingly rely on cyber-physical systems such as Global Navigation Satellite Systems (GNSS), Automatic Identification Systems (AIS), Electronic Chart Display and Information Systems (ECDIS), Software-Defined Radios (SDRs), and cloud-enabled fleet management platforms. While these technologies improve efficiency and situational awareness, they also expose maritime operations to a growing and increasingly sophisticated cyber threat landscape.

Recent real-world incidents—including GPS spoofing campaigns, AIS manipulation, ransomware attacks on shipping companies, and denial-of-service disruptions of port infrastructure—demonstrate that maritime cyber threats are no longer hypothetical. The flexibility and reconfigurability of SDR technologies, now embedded across maritime communication and navigation systems, further amplify these risks by enabling low-cost, high-impact radio-frequency attacks that bypass traditional IT-centric security controls. Research has shown that these threats are multidimensional, interdependent, and capable of cascading across device, software, network, and human layers, directly impacting vessel safety, operational continuity, and global supply chains [1].

Despite increasing regulatory attention, cybersecurity preparedness across the maritime sector remains uneven, particularly among small-to-medium sized organizations. Many operators lack standardized, maritime-specific methodologies for assessing cyber risk and instead rely on generic IT frameworks that fail to capture RF-layer attacks, SDR exploitation, and cyber-physical safety implications. *This paper addresses that gap by proposing a comprehensive, data-driven cybersecurity risk assessment approach tailored specifically to small-to-medium sized maritime transportation organizations. The approach leverages empirical insights from the Maritime Cyber Attack Database (MCAD) and integrates current research on maritime SDR vulnerabilities to provide actionable, operationally relevant guidance for private-sector stakeholders.*

Contents

1. Introduction

1.1 Maritime Digitalization and Cyber Dependency

Maritime transportation remains one of the most complex and safety-critical operational environments in the global economy. The sector's increasing reliance on digital technologies has fundamentally changed how vessels navigate, communicate, and interact with port and logistics ecosystems. Navigation accuracy, collision avoidance, cargo tracking, weather routing, and regulatory compliance are now tightly coupled with continuous access to digital data streams. Modern vessels operate as mobile cyber-physical systems, integrating navigation sensors, radio communications, onboard networks, satellite links, and shore-based services into a single operational environment. Software-Defined Radio technology has emerged as a key enabler in this ecosystem, allowing ships to support multiple communication protocols, dynamically adapt to changing spectrum conditions, and maintain interoperability across heterogeneous maritime networks. SDRs are now embedded in systems supporting GNSS reception, AIS transmission and reception, VHF and Digital Selective Calling (DSC), radar integration, and emerging maritime data exchange services. However, this digital convergence has also collapsed traditional security boundaries. Maritime systems that were once isolated are now interconnected across radio, network, and cloud domains. As demonstrated in recent research, SDRs operate at the intersection of hardware, software, and spectrum, creating a uniquely complex risk profile that differs fundamentally from conventional IT or industrial control environments [2]. Compromise at any layer—signal, firmware, protocol, or management interface—can propagate across navigation, communication, and safety systems.

1.2 Current Cyber Threat Reality in the Maritime Sector

The maritime cyber threat landscape has evolved rapidly in both scale and sophistication. Attackers no longer require nation-state resources to interfere with maritime systems. Commodity SDR hardware, open-source toolchains, and publicly documented protocol specifications have significantly lowered the barrier to entry for adversaries. As a result, cyber threats now originate from a broad spectrum of actors, including criminal groups, hacktivists, insiders, and state-aligned entities.

Documented incidents illustrate several recurring threat patterns:

- GNSS and GPS spoofing, where counterfeit satellite signals mislead vessels regarding their true position and time.
- AIS manipulation, enabling the creation of ghost vessels, identity spoofing, or the suppression of legitimate traffic.
- Denial-of-service attacks, including RF jamming and protocol-aware flooding, that disrupt navigation and communication.
- Tampering and privilege escalation, exploiting SDR firmware and management interfaces to gain persistent control.
- Information disclosure, through passive interception of unencrypted maritime broadcasts.

These threats are not isolated technical events; they directly impact vessel safety, cargo integrity, insurance liability, environmental risk, and regulatory compliance. The attached study systematically demonstrates that maritime SDR threats are multidimensional and interdependent, with attacks at the RF or protocol layer cascading into broader operational failures [3].

1.3 The Role of Empirical Incident Data

While academic research has extensively analyzed maritime cyber vulnerabilities, many private-sector risk assessments remain disconnected from real-world incident data. The Maritime Cyber Attack Database (MCAD) provides a unique empirical foundation for understanding how cyber threats materialize in practice. MCAD is a publicly accessible repository documenting over 160 maritime cyber incidents since 2001, compiled using open-source intelligence and public disclosures. The database captures a wide range of events, from ransomware attacks on shipping companies to GPS spoofing campaigns affecting naval and commercial vessels. One of the most cited cases occurred in 2021, when GPS spoofing activity altered the reported locations of NATO ships operating in the Black Sea near Ukraine. Such incidents illustrate how cyber operations can directly influence maritime safety, geopolitical stability, and freedom of navigation. Despite the availability of this data, many maritime organizations do not systematically integrate historical incident analysis into their cybersecurity risk assessments. Instead, decisions are often based on generic threat lists, vendor claims, or compliance checklists. This disconnect leads to misaligned priorities and leaves critical vulnerabilities unaddressed.

1.4 Challenges Facing Small-to-Medium Maritime Organizations

Small-to-medium sized maritime organizations face unique cybersecurity challenges that differ from those of large multinational operators. These organizations often operate with:

- Limited cybersecurity staffing and budgets,
- Legacy navigation and communication equipment,
- Heavy reliance on third-party vendors and managed services,
- Minimal visibility into RF-layer threats and SDR exploitation.

At the same time, they are subject to the same operational risks, regulatory obligations, and insurance expectations as larger organizations. A single cyber incident can halt operations, delay cargo, or expose the organization to significant liability. Yet, most existing cybersecurity frameworks assume a level of technical maturity and resource availability that smaller operators simply do not possess.

1.5 Purpose and Scope of This Paper

The purpose of this paper is to bridge the gap between academic threat analysis and practical, industry-ready cybersecurity risk management for maritime transportation systems. Specifically, this paper aims to:

1. Translate current maritime cyber threat research - particularly SDR-enabled threats - into operational risk language relevant to private industry.
2. Leverage MCAD incident data to ground risk assessments in real-world evidence.
3. Propose a scalable, data-driven cybersecurity risk assessment framework tailored to small-to-medium maritime organizations.
4. Emphasize not only prevention but also resilience, response, and operational continuity.

The remainder of this paper is structured as follows:

Part 2 Presents a detailed gap assessment and problem statement.

Part 3 Examines the current maritime cyber threat landscape using MCAD and STRIDE-aligned threat categories.

Part 4 Introduces the proposed risk assessment framework and associated security controls.

Part 5 Discusses the way forward for industry adoption, resilience building, and future research directions.

2. Gap Assessment and Problem Statement

2.1 The Disconnect Between Cyber Threat Reality and Industry Practice

Despite growing awareness of cyber risks in maritime transportation, there remains a pronounced disconnect between documented cyber threats and how risk is assessed and managed in practice, particularly within small-to-medium sized maritime organizations. While recent research has rigorously analyzed maritime cyber vulnerabilities - especially those introduced by Software-Defined Radio (SDR) technologies - these insights have not been translated into widely adopted, operational risk assessment methodologies within private industry. Maritime cyber threats are multidimensional, interdependent, and capable of cascading across systems, yet most industry risk assessments continue to treat cybersecurity as an isolated IT concern rather than a core operational and safety risk [4]. This gap is especially dangerous in maritime environments, where cyber incidents can rapidly propagate into physical consequences such as navigational errors, collisions, port shutdowns, and environmental damage.

2.2 Limitations of Traditional IT-Centric Risk Models

Most maritime organizations rely on cybersecurity frameworks originally designed for enterprise IT environments. These frameworks emphasize perimeter defense, endpoint protection, and data confidentiality but fail to address the radio-frequency (RF) and cyber-physical dimensions of maritime systems.

Traditional IT-centric models exhibit several structural shortcomings when applied to maritime operations:

- RF-layer blind spots: GNSS, AIS, VHF, and DSC systems operate over open and shared spectrum, yet conventional risk assessments rarely evaluate signal spoofing, jamming, or waveform manipulation.
- Inadequate treatment of SDR risks: SDR platforms collapse hardware, software, and protocol layers into a single reconfigurable system. Attacks against SDR firmware or waveforms can bypass network-based defenses entirely.
- Neglect of safety-critical dependencies: In maritime contexts, cyber compromise does not merely result in data loss; it can undermine navigation, collision avoidance, and emergency response.
- Assumption of static infrastructure: Maritime systems are mobile, internationally distributed, and exposed to adversarial environments, unlike fixed enterprise networks.

SDR-enabled threats exploit these blind spots, enabling attackers to manipulate navigation and communication systems without ever touching traditional IT assets [5]. As a result, organizations relying solely on IT-centric risk assessments underestimate both the likelihood and severity of maritime cyber incidents.

2.3 Overreliance on Compliance-Driven Approaches

Another critical gap lies in the industry's reliance on compliance-driven cybersecurity practices. Regulatory frameworks issued by bodies such as the International Maritime Organization (IMO) and national authorities have been instrumental in raising awareness. However, these frameworks are intentionally high-level, focusing on governance and policy integration rather than technical threat modeling. For many organizations - especially smaller operators - compliance has become the de facto goal of cybersecurity. Risk assessments are often conducted to satisfy audit requirements rather than to meaningfully understand and mitigate operational risk. This results in:

- Checklist-based assessments that do not reflect real attack scenarios,
- Minimal prioritization of risks based on likelihood and impact,
- Limited investment in detection, response, and resilience capabilities.

In [6], the authors highlight that significant gaps persist in authentication mechanisms, protocol integrity, and standardized forensic procedures across maritime systems. Compliance alone does not address these gaps, nor does it help organizations decide which risks matter most in practice.

2.4 Underutilization of Empirical Incident Evidence

The maritime sector is not lacking in incident data. The Maritime Cyber Attack Database (MCAD) documents more than 160 cyber incidents affecting maritime systems since 2001, covering a wide range of threat actors, attack techniques, and operational impacts. These incidents include ransomware attacks on shipping companies, GPS spoofing campaigns affecting commercial and military vessels, AIS manipulation, and port system breaches. Yet this empirical evidence is rarely integrated into formal risk assessment processes. Instead, many organizations rely on generic threat catalogs or vendor-provided risk narratives. This underutilization of historical incident data leads to several consequences:

- Misjudged likelihood: Rare but highly publicized attacks may receive disproportionate attention, while common attack patterns documented in MCAD are overlooked.
- Incomplete impact analysis: Without studying real incidents, organizations fail to appreciate how cyber events propagate across navigation, logistics, and safety systems.
- Reactive security posture: Controls are often deployed only after incidents occur elsewhere, rather than proactively based on observed trends.

Many maritime SDR threats have been repeatedly demonstrated in both empirical and simulation studies yet remain insufficiently addressed in operational environments [7].

2.5 Disproportionate Risk Exposure for Small-to-Medium Organizations

Small-to-medium sized maritime organizations face a particularly acute version of the cybersecurity problem. These organizations typically operate under constraints that include limited budgets, minimal cybersecurity expertise, and reliance on legacy equipment. At the same time, they are increasingly integrated into digital supply chains and subject to the same threat landscape as larger operators.

Several structural factors exacerbate their risk exposure:

- Legacy navigation and communication systems that lack authentication or encryption,
- Limited RF monitoring capabilities, making spoofing and jamming difficult to detect,
- Vendor dependency, where security is assumed rather than verified,
- Absence of formal incident response planning, particularly for cyber-physical scenarios.

Maritime SDR threats often exploit exactly these conditions—weak authentication, unsecured firmware, and limited monitoring—to achieve persistent and stealthy compromise [8]. For smaller organizations, even a single successful attack can result in prolonged downtime, contractual penalties, and reputational damage.

2.6 Inadequate Integration of Safety, Security, and Operations

A defining characteristic of maritime cyber risk is its direct relationship to safety and operational continuity. However, many organizations continue to treat cybersecurity as a separate discipline from navigation safety, engineering, and operations. This separation creates organizational silos that hinder effective risk management.

In practice:

- Navigation officers may not be trained to recognize cyber-induced anomalies,
- IT teams may lack understanding of navigational dependencies,
- Incident response plans may not account for degraded-mode navigation or manual operations.

Attacks such as GNSS spoofing and AIS manipulation can directly undermine situational awareness and collision avoidance [9]. Without integrated safety–security thinking, organizations are ill-prepared to respond when cyber incidents manifest as navigational failures.

2.7 Lack of Resilience-Oriented Risk Assessment

Finally, existing risk assessment approaches place insufficient emphasis on resilience and recovery. While prevention is important, the maritime environment makes complete prevention unrealistic. Open-spectrum communication, legacy protocols, and international operating conditions ensure that some level of exposure will persist. Nganga et al. [10] highlights the need for proactive security engineering, adaptive spectrum management, and standardized forensic procedures to ensure resilience and trustworthiness in maritime operations. However, most risk assessments do not evaluate an organization’s ability to:

- Detect cyber anomalies in real time,
- Continue operations during partial system failure,
- Recover safely and efficiently after an incident.

This omission leaves organizations vulnerable not only to initial compromise but also to prolonged operational disruption.

2.8 Problem Statement

In summary, the core problem facing the maritime industry - particularly small-to-medium sized organizations - is not a lack of awareness of cyber threats, but a lack of practical, data-driven, maritime-specific risk assessment methodologies. Existing approaches fail to:

1. Capture RF-layer and SDR-enabled attack vectors,
2. Leverage empirical incident data such as MCAD,
3. Reflect the safety-critical and cyber-physical nature of maritime operations,
4. Address the resource constraints of smaller organizations,
5. Integrate resilience and recovery into risk evaluation.

Addressing these gaps requires a shift from compliance-driven, IT-centric assessments toward evidence-based, operationally grounded cybersecurity risk management. The next section builds on this problem statement by examining the current maritime cyber threat landscape in detail, using MCAD data and SDR-focused threat modeling to establish a foundation for the proposed risk assessment framework.

3. Topic Discussion: Current Maritime Cyber Threat Landscape

3.1 Overview of the Modern Maritime Cyber Threat Environment

The contemporary maritime cyber threat landscape is shaped by the convergence of digitalization, increased automation, and widespread adoption of wireless communication technologies. Unlike traditional enterprise environments, maritime systems operate in open, shared, and often contested electromagnetic environments, making them particularly vulnerable to cyber-attacks that exploit radio frequency (RF) and protocol-level weaknesses. The increasing reliance on Software-Defined Radio (SDR) technologies amplifies this exposure by enabling reconfigurable signal processing and protocol flexibility at relatively low cost. Analysis of incidents documented in the Maritime Cyber Attack Database (MCAD), combined with recent academic research, demonstrates that maritime cyber threats are not isolated or single-layered. Instead, they are systemic, often exploiting multiple layers simultaneously—signal, protocol, software, and human—to achieve operational impact. These threats directly affect vessel navigation, situational awareness, port operations, cargo handling, and safety-critical decision-making. A defining characteristic of maritime cyber threats is their cyber-physical nature. Successful attacks frequently result in physical consequences, such as misdirected vessels, delayed cargo, collisions, or environmental incidents. This reality distinguishes maritime cybersecurity from conventional IT security and necessitates a threat analysis approach grounded in operational risk rather than abstract technical vulnerabilities.

3.2 Empirical Threat Trends from MCAD

The MCAD dataset provides valuable insight into how maritime cyber threats have evolved over time. Since its earliest recorded incidents in the early 2000s, the database shows a steady increase in both the frequency and sophistication of attacks. Early incidents were often limited to isolated system compromises or rudimentary jamming. In contrast, recent incidents demonstrate coordinated, multi-stage attacks that leverage both cyber and RF techniques.

Several trends emerge from MCAD analysis:

- Persistent exploitation of unauthenticated protocols, particularly GNSS and AIS.
- Increased use of spoofing and deception, rather than purely destructive attacks.
- Growing overlap between cybercrime and geopolitical activity, especially in contested maritime regions.
- Rising impact of attacks on logistics and port operations, not just vessels at sea.

These trends indicate that attackers increasingly favor methods that are difficult to attribute, difficult to detect, and capable of producing operational disruption without overt system destruction.

*The following sections discuss the threat trends in a sequence following the Microsoft-developed threat modeling framework of STRIDE: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, and **E**levation of Privilege.*[1]

3.3 Spoofing Attacks: Deception as a Primary Threat Vector

Spoofing represents one of the most significant and well-documented threat categories in the maritime domain. Spoofing attacks involve transmitting falsified signals or messages that appear legitimate to victim systems, causing them to accept incorrect information as true. In maritime environments, spoofing primarily targets GNSS, AIS, VHF, and associated navigation data streams.

3.3.1 GNSS and GPS Spoofing

GNSS spoofing has emerged as a dominant threat due to the maritime sector's heavy reliance on satellite-based positioning and timing. Using SDR platforms, attackers can generate counterfeit satellite signals that cause receivers to calculate false positions or time offsets. These attacks can be executed gradually to avoid detection, resulting in subtle navigational deviations that may go unnoticed until operational consequences arise.

MCAD records multiple incidents where vessels reported implausible positions, including sudden relocations to airports or inland areas. The 2021 Black Sea incident involving spoofed locations of NATO vessels exemplifies the strategic use of GNSS spoofing to create navigational uncertainty without physical confrontation.

From an operational perspective, GNSS spoofing undermines:

- Route planning and collision avoidance,
- ECDIS accuracy,
- Time synchronization for communication and logging systems,
- Trust in automated navigation aids.

3.3.2 AIS Spoofing and Ghost Vessels

AIS spoofing enables attackers to fabricate vessel identities, manipulate position reports, or suppress legitimate traffic. Using SDRs, adversaries can transmit protocol-compliant AIS messages that create "ghost vessels," alter reported vessel speed or heading, or impersonate legitimate ships.

[1] Chris Romeo, August 25, 2025, What is STRIDE in Threat Modeling? https://www.securitycompass.com/blog/stride-in-threat-modeling/#:~:text=STRIDE%20is%20a%20threat%20modeling,%E2%80%9CWhat%20can%20go%20wrong?%E2%80%9D

Such attacks have been used to:

- Obscure illegal activities,
- Confuse vessel traffic services,
- Manipulate maritime domain awareness systems,
- Create false congestion or collision risks.

AIS spoofing is particularly dangerous because it exploits a system originally designed for safety and transparency, turning it into a vector for deception.

3.4 Tampering Attacks: Manipulating Systems from Within

Tampering attacks involve unauthorized modification of systems, firmware, or data streams. In SDR-enabled maritime environments, tampering can occur at multiple levels, including waveform generation, firmware configuration, and protocol processing.

3.4.1 SDR Firmware and Configuration Tampering

SDR platforms are particularly susceptible to tampering due to their programmable nature [11]. Attackers who gain access to SDR firmware or control interfaces can modify signal behavior, inject malicious waveforms, or persistently alter system functionality.

Such tampering may enable:

- Long-term spoofing without continuous external transmission,
- Covert jamming or interference,
- Hidden backdoors for future access.

For maritime operators, compromised SDR components represent a latent risk that may remain undetected until triggered.

3.4.2 Data Stream and Protocol Tampering

Tampering also occurs through manipulation of data streams such as NMEA sentences, AIS messages, or sensor inputs. By altering these data flows, attackers can influence navigation displays, alarm systems, and automated decision-support tools.

Operational consequences include:

- Incorrect chart updates,
- False collision warnings,
- Misinterpretation of vessel status,
- Compromised safety management systems.

3.5 Repudiation: Undermining Accountability and Forensics

Repudiation threats arise when actions cannot be reliably attributed due to weak logging, lack of authentication, or tamperable records. Maritime systems frequently lack cryptographic non-repudiation mechanisms, making forensic investigation challenging.

Attackers may:

- Delete or alter logs,
- Replay legitimate messages to obscure timelines,
- Exploit ambiguous system behavior to deny responsibility.

From an industry perspective, repudiation undermines:

- Incident investigation,
- Insurance claims,
- Regulatory compliance,
- Legal accountability.

3.6 Information Disclosure: Passive Exploitation of Open Systems

Information disclosure attacks exploit the open nature of maritime communication systems. Many maritime protocols broadcast unencrypted data by design, allowing passive interception by anyone with basic SDR equipment.

3.6.1 Passive Eavesdropping and Traffic Analysis

AIS broadcasts expose vessel identity, position, speed, and voyage information. When combined with external data sources, attackers can reconstruct operational patterns, infer cargo movements, or track sensitive activities.

MCAD incidents show that such data has been used for:

- Competitive intelligence,
- Target selection for physical or cyber-attacks,
- Surveillance of military or government vessels.

3.6.2 Aggregation and Inference Risks

Even when individual data points appear benign, aggregation across time and sources can reveal sensitive operational insights. This risk is particularly relevant for small operators who may assume that “public” data poses no security concern.

3.7 Denial-of-Service Attacks: Disrupting Availability

Denial-of-service (DoS) attacks target the availability of maritime systems, preventing legitimate use of navigation or communication services. In maritime environments, DoS attacks often exploit RF channels rather than traditional network traffic.

3.7.1 RF Jamming and Interference

RF jamming involves overwhelming receivers with noise or interfering signals, preventing them from receiving legitimate transmissions. GNSS jamming, in particular, has been documented extensively in MCAD and recent research.

Jamming attacks may be:

- Localized and temporary,
- Mobile and difficult to trace,
- Coordinated across multiple vessels or ports.

Even short-term jamming can force vessels to revert to degraded navigation modes, increasing operational risk.

3.7.2 Protocol-Aware Flooding

In addition to raw RF jamming, attackers may flood AIS or VHF channels with valid-looking messages, overwhelming receivers and human operators alike. Such attacks degrade situational awareness without obvious signs of malicious intent.

3.8 Elevation of Privilege: Gaining Persistent Control

Elevation-of-privilege attacks enable attackers to move from limited access to full control of systems. In maritime environments, this may involve exploiting vulnerabilities in SDR management interfaces, onboard networks, or gateway devices.

Once elevated privileges are obtained, attackers can:

- Install persistent malware,
- Modify navigation or communication behavior,
- Disable monitoring and logging,
- Pivot between vessel and shore-based systems.

Privilege escalation in SDR ecosystems enables long-term compromise with minimal visibility [12].

3.9 Operational Impact and Industry Implications

Across all threat categories, a consistent theme emerges: maritime cyber-attacks prioritize deception, persistence, and operational disruption over immediate destruction. This strategy aligns with attackers’ desire to remain undetected while influencing navigation, logistics, or geopolitical outcomes.

For private industry, the implications are profound:

- Cyber incidents directly affect safety and liability,
- Detection is often delayed or uncertain,
- Recovery requires coordinated technical and operational response.

These realities underscore the need for a cybersecurity risk assessment approach that is grounded in real-world threat behavior, operational context, and empirical incident data.

3.10 Summary of Threat Landscape Findings

In summary, the current maritime cyber threat landscape is characterized by:

- High prevalence of spoofing, tampering, and DoS attacks,
- Exploitation of SDR flexibility and RF-layer vulnerabilities,
- Persistent weaknesses in authentication and protocol integrity,
- Direct coupling of cyber events to physical and safety outcomes.

These findings establish the foundation for the next section, which presents a practical, data-driven cybersecurity risk assessment framework designed to help small-to-medium maritime organizations prioritize risks, deploy appropriate controls, and enhance resilience.

4. Topic Discussion: A Practical Cybersecurity Risk Assessment Framework for Maritime Transportation Systems

4.1 Rationale for a Maritime-Specific, Data-Driven Framework

The threat analysis presented in Part 3 demonstrates that maritime cyber risks differ fundamentally from those encountered in traditional enterprise IT environments. Attacks exploit radio-frequency channels, software-defined radio platforms, legacy maritime protocols, and human–machine interactions in ways that are not adequately captured by conventional risk assessment methodologies. Consequently, maritime organizations (particularly small-to-medium sized operators) require a purpose-built cybersecurity risk assessment framework that reflects operational realities, safety dependencies, and empirical threat behavior.

The proposed framework addresses this need by integrating:

- Empirical incident evidence from the Maritime Cyber Attack Database (MCAD),
- Threat modeling insights derived from SDR-focused research,
- Operational impact analysis aligned with maritime safety and continuity requirements,
- Scalable implementation guidance suitable for organizations with limited resources.

Rather than replacing existing standards or regulations, this framework complements them by translating high-level guidance into concrete, operationally actionable steps.

4.2 Framework Design Principles

The framework is guided by five core principles that reflect both maritime operational constraints and the findings of recent cyber threat research:

1. Evidence-based prioritization: Risks are evaluated using real-world incident patterns from MCAD rather than hypothetical threat lists.
2. Cyber-physical integration: Cybersecurity risks are assessed in terms of their impact on navigation, safety, and operations, not solely on their information confidentiality.
3. Layered threat visibility: Threats are evaluated across signal, protocol, software, network, and human layers, reflecting SDR-enabled attack paths.
4. Scalability and feasibility: Controls are prioritized based on effectiveness and practicality for small-to-medium organizations.
5. Resilience over perfection: The framework emphasizes detection, response, and recovery, acknowledging that complete prevention is unrealistic in open maritime environments.

4.3 Framework Structure Overview

The proposed cybersecurity risk assessment framework consists of four interrelated phases (Figure 1):

1. Asset and Operational Context Definition
2. Threat and Vulnerability Identification
3. Risk Analysis and Prioritization
4. Control Selection, Implementation, and Resilience Planning

4.4 Phase 1: Asset and Operational Context Definition

4.4.1 Identifying Critical Maritime Assets

Effective risk assessment begins with a clear understanding of what must be protected. In maritime environments, critical assets extend beyond traditional IT systems and include:

- Navigation systems (GNSS receivers, ECDIS, radar integration),
- Communication systems (AIS, VHF, DSC, satellite links),
- SDR platforms and embedded radio modules,
- Shipboard networks and gateways,
- Port and shore-based systems (VTS, terminal operating systems),
- Human operators and decision-making processes.

Organizations should classify assets based on their role in safety, operations, compliance, and business continuity.

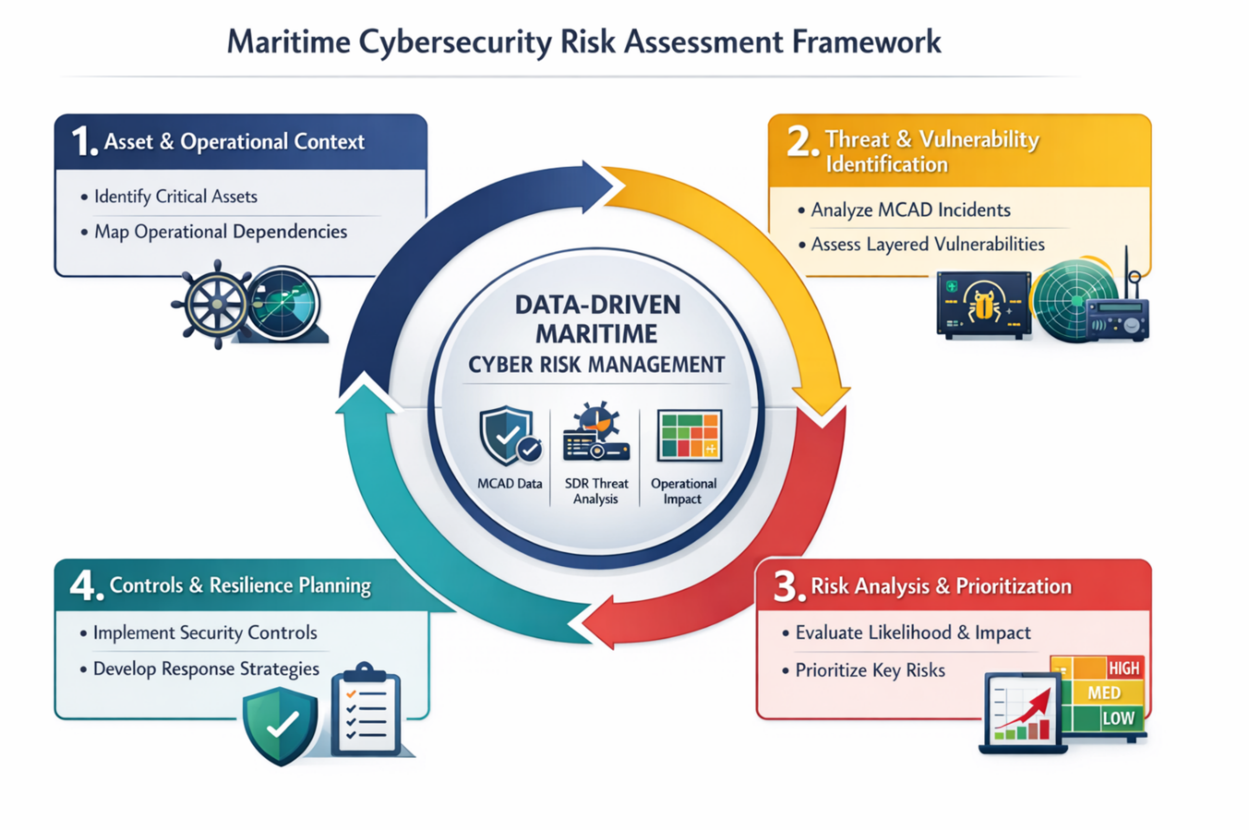
Maritime Cybersecurity Risk Assessment Framework
1. Asset & Operational Context
• Identify Critical Assets
• Map Operational Dependencies
2. Threat & Vulnerability Identification
• Analyze MCAD Incidents
• Assess Layered Vulnerabilities
DATA-DRIVEN MARITIME CYBER RISK MANAGEMENT
MCAD Data
SDR Threat Analysis
Operational Impact
3. Risk Analysis & Prioritization
• Evaluate Likelihood & Impact
• Prioritize Key Risks
HIGH
MED
LOW
4. Controls & Resilience Planning
• Implement Security Controls
• Develop Response Strategies

Figure 1: Cybersecurity Framework

4.4.2 Operational Dependency Mapping

Next, dependencies between assets must be mapped. For example, GNSS feeds influence ECDIS, AIS, time synchronization, and voyage data recorders. SDR platforms may support multiple protocols simultaneously, creating single points of failure. Mapping these dependencies helps organizations understand how cyber incidents propagate across systems - a phenomenon repeatedly observed in documented maritime cyber attacks [4].

4.5 Phase 2: Threat and Vulnerability Identification

4.5.1 Leveraging MCAD for Threat Identification

Rather than relying solely on generic threat catalogs, organizations should use MCAD to identify the most relevant threat categories based on historical frequency, geographic location, and potential impact.

Common MCAD-aligned threats include:

- GNSS and AIS spoofing,
- SDR firmware and waveform tampering,
- RF jamming and denial-of-service,
- Unauthorized access and privilege escalation,
- Passive eavesdropping and information disclosure.

This evidence-based approach ensures that risk assessments reflect realistic attack scenarios rather than speculative threats.

4.5.2 Vulnerability Identification Across Layers

Vulnerabilities should be assessed across five layers:

1. Signal layer: susceptibility to spoofing, jamming, interference.
2. Protocol layer: lack of authentication, encryption, integrity checks.
3. Software/Firmware layer: insecure SDR firmware, update mechanisms, parsers.
4. Network layer: flat networks, weak segmentation, exposed interfaces.
5. Human layer: limited training, overreliance on automated systems.

The research demonstrates that attacks often traverse multiple layers, exploiting weak links to achieve operational impact [4].

4.6 Phase 3: Risk Analysis and Prioritization

4.6.1 Likelihood Assessment

Likelihood is estimated using MCAD incident frequency, demonstrated attack feasibility, and environmental exposure. For example:

- GNSS spoofing has high likelihood in open or contested waters,
- AIS spoofing is feasible wherever unencrypted broadcasts are relied upon,
- SDR tampering likelihood increases with unmanaged firmware and vendor dependency.

Organizations should adjust likelihood estimates based on operational context, geography, and asset exposure.

4.6.2 Impact Assessment

Impact is assessed across multiple dimensions:

- Safety impact: collision risk, grounding, loss of situational awareness,
- Operational impact: voyage delays, port shutdowns, degraded navigation,
- Financial impact: lost revenue, recovery costs, insurance implications,
- Regulatory impact: non-compliance, audit findings, legal exposure,
- Reputational impact: loss of customer trust and market position.

This multi-dimensional impact assessment reflects the cyber-physical nature of maritime risk.

4.6.3 Risk Prioritization

Risks are prioritized by combining likelihood and impact scores, enabling organizations to focus resources on the most consequential threats. For small-to-medium operators, this prioritization is essential to avoid spreading limited resources too thinly.

4.7 Phase 4: Control Selection and Implementation

4.7.1 Preventive Controls

Preventive controls aim to reduce attack success probability and include:

- Secure configuration and firmware signing for SDR platforms,
- Network segmentation between navigation, OT, and IT systems,
- Access control and credential management for onboard and shore systems,
- Vendor security assessment and update verification.

While prevention is important, it must be balanced against operational feasibility.

4.7.2 Detection and Monitoring Controls

Given the prevalence of stealthy attacks such as spoofing and tampering, detection is critical. Recommended controls include:

- GNSS anomaly detection and multi-sensor cross-checking,
- AIS and VHF traffic monitoring for implausible patterns,
- SDR telemetry and configuration integrity monitoring,
- Centralized logging and time synchronization for forensic analysis.

These controls help reduce dwell time and enable timely response.

4.7.3 Response and Resilience Measures

Resilience-focused controls prepare organizations to operate safely during and after cyber incidents:

- Degraded-mode navigation procedures (radar, visual fixes),
- Cyber incident playbooks tailored to maritime scenarios,
- Crew training to recognize cyber-induced anomalies,
- Backup communication and navigation capabilities.

The attached research emphasizes that resilience and adaptive response are essential given persistent protocol and SDR vulnerabilities [13].

4.8 Integrating the Framework into Existing Operations

To maximize adoption, the framework should be integrated into existing safety management systems (SMS), operational procedures, and maintenance cycles. Cyber risk assessment should become a recurring process, updated as new MCAD incidents and threat intelligence emerge. For small-to-medium organizations, incremental adoption—starting with high-risk assets and threats—is both practical and effective.

4.9 Summary of Framework Benefits

The proposed framework provides several benefits to private maritime industry stakeholders:

- Grounding risk assessment in real-world incident evidence,
- Addressing SDR-enabled and RF-layer threats explicitly,
- Aligning cybersecurity with safety and operational continuity,
- Supporting scalable implementation under resource constraints,
- Shifting focus from compliance to meaningful risk reduction.

This framework sets the stage for the final section, which discusses the way forward for industry adoption, collaboration, and long-term maritime cyber resilience.

5. Way Forward: Building Sustainable Cyber Resilience in Maritime Transportation Systems

5.1 From Awareness to Operational Cyber Risk Management

The preceding sections have demonstrated that cybersecurity in maritime transportation systems is no longer a peripheral IT concern but a core operational and safety risk. Empirical evidence from the Maritime Cyber Attack Database (MCAD), combined with recent research on Software-Defined Radio (SDR) vulnerabilities, reveals a threat landscape characterized by deception, persistence, and cyber-physical impact. These threats directly affect navigation accuracy, situational awareness, port operations, and supply chain continuity. The way forward for the maritime industry requires a decisive shift from awareness-driven cybersecurity toward operationally embedded cyber risk management. This transition involves moving beyond compliance checklists and ad hoc controls to a systematic, data-driven approach that prioritizes real-world threats, operational dependencies, and resilience outcomes. For private-sector stakeholders, the question is no longer whether cyber incidents will occur, but how effectively organizations can detect, respond to, and recover from them while maintaining safe and reliable operations.

5.2 Embedding Cybersecurity into Maritime Safety Culture

A critical element of sustainable maritime cyber resilience is the integration of cybersecurity into existing maritime safety culture. Traditionally, safety management in maritime operations has focused on mechanical reliability, human error, and environmental hazards. However, cyber threats now intersect with all three domains. Organizations should explicitly recognize cybersecurity as a contributor to navigational and operational risk. This recognition must extend beyond IT departments to include bridge officers, engineers, port operators, and shore-based management. Practical steps include:

- Incorporating cyber scenarios into safety drills and training exercises,
- Educating crews on how cyber incidents may manifest as navigational anomalies rather than system failures,
- Ensuring that safety management systems (SMS) account for degraded-mode operations during cyber disruptions.

By embedding cybersecurity into safety culture, organizations reduce the likelihood that cyber-induced anomalies will be misinterpreted or ignored during critical decision-making moments.

5.3 Operationalizing the Risk Assessment Framework

For small-to-medium sized maritime organizations, successful adoption of the proposed cybersecurity risk assessment framework requires pragmatism and prioritization. The framework is intentionally designed to be incremental and scalable, allowing organizations to begin with the most critical assets and highest-risk threats.

Key steps for operationalization include:

1. Start with high-impact assets such as GNSS receivers, ECDIS, AIS, and SDR platforms that directly affect navigation and safety.
2. Leverage MCAD insights to focus on the most common and impactful attack types, rather than attempting to address all conceivable threats.
3. Align cybersecurity assessments with operational cycles, such as dry dock periods, audits, or safety reviews.
4. Document assumptions and limitations, acknowledging areas where detection or prevention capabilities remain constrained.

This incremental approach enables organizations to demonstrate measurable risk reduction without overwhelming limited resources.

5.4 Strengthening Detection, Response, and Recovery Capabilities

Given the open and contested nature of maritime communication environments, complete prevention of cyber attacks is unrealistic. As highlighted throughout this paper, many maritime protocols lack authentication and integrity protections by design, and SDR flexibility enables attackers to adapt rapidly.

Therefore, future maritime cybersecurity strategies must emphasize:

- Early detection of anomalies through signal analysis, cross-sensor validation, and behavioral monitoring,
- Prepared response, including predefined playbooks for spoofing, jamming, ransomware, and insider incidents,
- Rapid recovery, ensuring that vessels and ports can resume safe operations even under degraded conditions.

Organizations that invest in detection and resilience consistently outperform those focused solely on perimeter defenses, particularly in environments where attacks are subtle and attribution is difficult.

5.5 Industry Collaboration and Information Sharing

Maritime cybersecurity is inherently a collective challenge. Vessels, ports, logistics providers, insurers, and regulators operate within tightly coupled ecosystems where the vulnerability of one actor can affect many others. No single organization, especially small-to-medium sized operators, can maintain complete visibility into emerging threats on its own.

The way forward requires enhanced collaboration and information sharing, including:

- Broader participation in incident reporting initiatives such as MCAD,
- Sharing of anonymized threat indicators and lessons learned,
- Collaboration between industry, academia, and technology providers to validate mitigation strategies.

Improved information sharing not only strengthens individual organizations but also raises the baseline security posture of the entire maritime sector.

5.6 Implications for Insurers, Regulators, and Technology Providers

The findings of this paper have important implications beyond vessel operators and port authorities. Maritime insurers increasingly assess cyber risk when underwriting policies, and empirical, data-driven risk assessments can support more accurate pricing and coverage decisions. Organizations that demonstrate structured risk management and resilience capabilities may benefit from improved insurability and reduced premiums. Regulators, meanwhile, can use insights from MCAD and SDR-focused research to refine guidance and standards, moving beyond high-level principles toward more operationally relevant recommendations. Encouraging standardized incident reporting and risk assessment practices will improve regulatory oversight without imposing undue burden on industry. Technology providers, particularly those developing SDR-enabled maritime systems, bear a shared responsibility to address security by design. Improved authentication, firmware integrity, logging, and update mechanisms can significantly reduce systemic risk across the maritime ecosystem.

5.7 Future Research and Continuous Improvement

Maritime cybersecurity is not a static problem. Advances in automation, autonomous vessels, and digital port infrastructure will introduce new dependencies and attack surfaces.

Future research should focus on:

- Improving GNSS authentication and resilience techniques,
- Developing standardized forensic and logging mechanisms for maritime systems,
- Enhancing anomaly detection using machine learning and multi-sensor fusion,
- Evaluating the security implications of autonomous and remotely operated vessels.

Continuous integration of new research findings and incident data into risk assessment frameworks will be essential to maintaining long-term resilience.

5.8 Concluding Remarks

This paper has presented a comprehensive, data-driven cybersecurity risk assessment approach tailored to the realities of modern maritime transportation systems. By grounding analysis in empirical incident evidence from the Maritime Cyber Attack Database and integrating current research on SDR-enabled threats, the proposed framework bridges the gap between academic insight and industry practice. For private maritime organizations, particularly small-to-medium sized operators, the path forward lies in adopting pragmatic, evidence-based risk management strategies that align cybersecurity with safety, operations, and business continuity. As maritime systems continue to evolve in complexity and connectivity, those organizations that proactively embed cybersecurity into their operational fabric will be best positioned to navigate the digital future safely, securely, and sustainably.

6. REFERENCES

[1] S. Lee et al., "Securing Maritime Autonomous Surface Ships: Cyber Threat Scenarios and Testbed Validation," *IEEE Access*, vol. 13, pp. 10311-10325, 2025, doi: 10.1109/access.2025.3527132.

[2] N. Niknami, A. Srinivasan, and J. Wu, "Maritime Communications—Current State and the Future Potential with SDN and SDR," *Network*, vol. 3, no. 4, pp. 563–584, Dec. 2023, doi: 10.3390/network3040026

[3] A. Oruc, G. Kavallieratos, V. Gkioulos, and S. Katsikas, "Perspectives on the Cybersecurity of the Integrated Navigation System," *Journal of Marine Science and Engineering*, vol. 13, no. 6, Art. no. 1087, May 2025, doi: 10.3390/jmse13061087.

[4] E. Mfodwo, P. Lanka, A. F. Aydogan, and C. Varol, "Uncovering the Security Landscape of Maritime Software-Defined Radios: A Threat Modeling Perspective," *Applied Sciences*, vol. 16, no. 2, Art. no. 813, Jan. 2026, doi: 10.3390/app16020813

[5] N. Nikitakos and I. Progoulakis, "Advanced Research in Shipping Informatics and Communications," *Journal of Marine Science and Engineering*, vol. 13, no. 5, Art. no. 951, May 2025, doi: 10.3390/jmse13050951

[6] J. Kalliovaara, J. Hallio, J. Väänänen, and T. Jokela, "Security Challenges in Commercial off-the-shelf Equipment Integration for Small Autonomous Vessels: A Security-by-Design Approach," *Journal of Physics: Conference Series*, vol. 2842, no. 1, Art. no. 012015, Oct. 2025, doi: 10.1088/1742-6596/2842/1/012015.

[7] M. Li, J. Zhou, S. Chattopadhyay, and M. Goh, "Maritime Cybersecurity: A Comprehensive Review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 1, pp. 412–435, Jan. 2025, doi: 10.1109/TITS.2024.3461285

[8] R. Anuja and J. Annrose, "End-to-end deep learning for smart maritime threat detection: an AE–CNN–LSTM-based approach," *Scientific Reports*, vol. 15, no. 1, Art. no. 24812, Oct. 2025, doi: 10.1038/s41598-025-12534397.

[9] A. Androjna and M. Perkovič, "Impact of Spoofing of Navigation Systems on Maritime Situational Awareness," *Transactions on Maritime Science*, vol. 10, no. 2, pp. 361–373, Oct. 2021, doi: 10.7225/toms.v10.n02.w08

[10] A. Nganga, J. Scanlan, M. Lützhöft, and S. Mallam, "Enabling cyber resilient shipping through maritime security operation center adoption: A human factors perspective," *Applied Ergonomics*, vol. 119, Art. no. 104312, Sep. 2024, doi: 10.1016/j.apergo.2024.104312.

[11] T. Wu, X. Zhou, and W. Fu, "Security issues in software-defined radio: a review," *Cybersecurity*, vol. 9, no. 1, Art. no. 19, Jan. 2026, doi: 10.1186/s42400-026-00312-x

[12] S. Kumawat, S. Kumar, S. Saini, and V. Sharma, "Unlocking Security Risks: Exploring Vulnerabilities in Software-Defined Radio with RTL-SDR," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 12, no. 4, pp. 2450–2456, Apr. 2024, doi: 10.22214/ijraset.2024.59984.

[13] M. S. Araujo, B. A. S. Machado, and F. U. Passos, "Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance," *Applied Sciences*, vol. 14, no. 5, Art. no. 2116, Mar. 2024, doi: 10.3390/app14052116.

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, Water/Wastewater and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Varol, Cihan (2026) Comprehensive Cybersecurity Risk Assessments for Maritime Transportation Systems. (Report No. 2026 - 1034). The Sam Houston State University Institute for Homeland Security.

Sam Houston State University