Maritime Cyber Threat White Paper 2026

February 19, 2026

CYTUR Inc.

CYTUR

Cyber Trust & Resilience for Maritime

Based on the 'Secure by Design' philosophy—which integrates security from the earliest design stages—CYTUR is a leading maritime cybersecurity specialist. We provide integrated management solutions and services that protect the entire ship lifecycle, including ordering, contracting, design, construction, sea trials, and operations.

True to our name, CYTUR (Cyber Trust & Resilience), we are dedicated to delivering cyber trust and resilience to the maritime industry as it steers through the waves of digital transformation.

2026 Maritime Cyber Threat White Paper: Data-Driven Maritime Defense Strategies

1. Purpose of Publication

The maritime industry today faces unprecedented cyber threats driven by the acceleration of digital transformation. However, due to the closed and specialized nature of maritime environments, finding reliable threat data and analytical resources remains a significant challenge.

This white paper aims to address this information disparity. Our goal is to empower maritime stakeholders to accurately understand sophisticated cyber threats and take proactive measures against them.

2. Key Content and Structure

This report is based on real-world data collected through CYTUR-TI, our specialized maritime cyber threat intelligence solution.

It provides an in-depth analysis of global maritime threat information and the latest trends from 2024 through 2025.

3. Message to Our Readers

Cybersecurity is more than just a defensive technology; it is a core competency that ensures the safe operation of smart ships and guarantees business continuity. In particular, to realize the 'Secure by Design' philosophy—where security is integrated from the design phase—accurate threat intelligence must be the starting point.

In a field where information is scarce, we hope this white paper serves as a practical roadmap, turning uncertainty into confidence and fostering a more secure maritime digital ecosystem. CYTUR remains committed to being a steadfast digital guardian for the maritime industry, consistently sharing valuable insights for a safer future.

Securing the Smart Maritime Era: The Critical Need for Specialized Maritime CTI

Maritime Digital Transformation (DX) and the Expanded Attack Surface

The maritime and shipbuilding industry is currently facing a massive wave of Digital Transformation (DX). With the emergence of smart ships, data traffic for vessel performance monitoring and predictive maintenance has grown exponentially.

However, this increased connectivity is a double-edged sword. As Operational Technology (OT) systems—which were once isolated—become closely integrated with onshore Information Technology (IT) networks via satellite communications, the attack surface available to cyber adversaries has expanded has expanded exponentially.

In particular, the continuous flow of data between land and sea has increased the likelihood of exposing security vulnerabilities. This now poses a direct threat to the safe navigation of vessels, moving beyond simple data breaches to risking human lives and assets at sea.

Limitations of General-Purpose CTI and the Absence of Maritime-Specific Intelligence

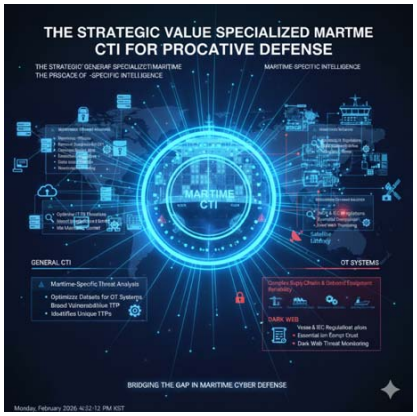
While many organizations currently rely on general-purpose Cyber Threat Intelligence (CTI) services, these services have clear limitations when applied to the unique characteristics of the maritime industry. General IT-based CTI is often insufficient

for analyzing security blind spots that emerge from the complex maritime supply chain—spanning shipbuilders, equipment manufacturers, and shipping companies—and the diverse range of onboard equipment.

Furthermore, threat analysis that fails to account for the unique maritime communication environment—such as satellite-specific latency and bandwidth constraints—cannot provide practical or effective response strategies. Of particular concern is the growing threat found in hidden areas like the Dark Web, where unauthorized access credentials for vessels and vulnerabilities in port operating systems are actively traded.

The Strategic Value of Specialized Maritime CTI for Proactive Defense

Specialized maritime CTI goes beyond simple intrusion detection; its primary goal is to enable proactive responses before a threat can materialize.



Maritime-Specific Threat Analysis

Based on datasets optimized for the maritime environment, it identifies unique threat patterns and Tactics, Techniques, and Procedures (TTPs) targeting shipboard OT systems.

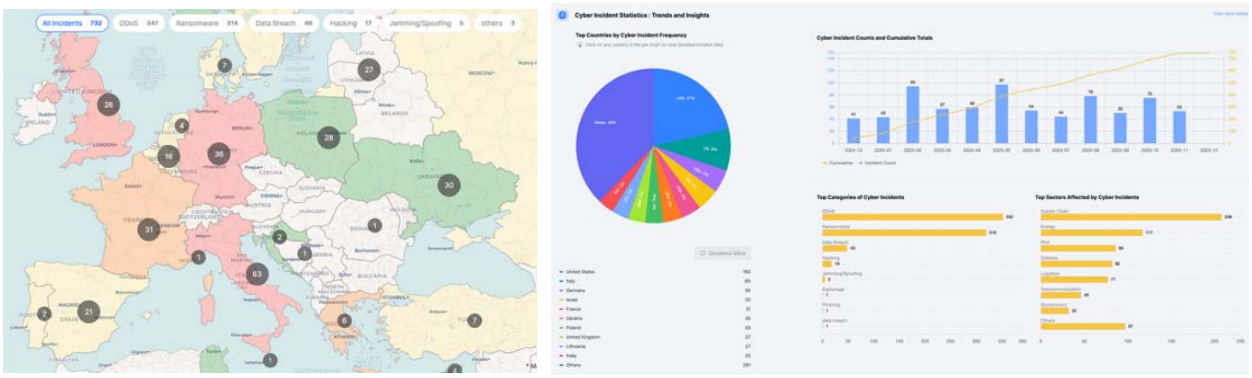
Regulatory Compliance and Reliability

As global cybersecurity regulations from organizations like the IMO (International Maritime Organization) and IEC continue to tighten, having reliable, specialized intelligence is essential for compliance.

Ultimately, the key to protecting vessels and assets in a shifting maritime threat landscape is securing "intelligence that speaks the language of the sea." Specialized maritime CTI is not merely a security tool; it is a strategic asset that ensures the safe operation of smart ships and the sustainability of the business.

CYTUR-TI(Threat Intelligence): Specialized Maritime Cyber Threat Intelligence

[Key Features and Advantages]



CYTUR-TI™

1. Maritime-Specific Threat Data Analysis

We analyze global maritime cyberattack cases and hacking group activities. Our intelligence is uniquely optimized for the maritime industry, focusing on the collection of vulnerability data regarding key maritime communication protocols (such as NMEA and AIS) and onboard Operational Technology (OT) systems.

2. Deep and Dark Web Monitoring

We provide real-time monitoring of hidden digital spaces inaccessible by standard search engines, including dark web forums, marketplaces, and encrypted messenger channels. This allows us to identify early warning signs directly linked to maritime assets, such as the sale of vessel access credentials, compromised crew accounts, and leaked ship design schematics. When a specific attack plan targeting a client's fleet or shipping company is detected, an immediate alert is issued to security officers, enabling an instantaneous reinforcement of security policies.

3. Synergistic Integration for Holistic Analysis

CYTUR-TI integrates seamlessly with CYTUR-NS and CYTUR-TA, which monitor real-time vessel status data. by cross-analyzing external Threat Intelligence (TI) with internal Operational Technology (OT) status information, the system can clearly distinguish whether a malfunction is a simple mechanical failure or a malicious disruption caused by an external cyberattack.

[Implementation Benefits and Business Value]

1. Enhanced Cyber Resilience

By blocking potential intrusion paths before an attacker can target vessel systems, we ensure the operational safety of ships and the continuity of your business.

2. Reduction in Remediation Costs

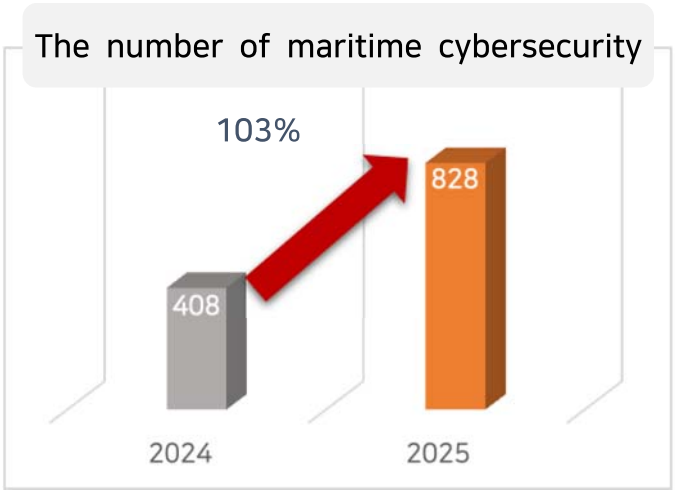
By shifting from a reactive "incident response" model to a proactive "threat detection" approach, we minimize the risk of astronomical recovery costs associated with large-scale data breaches or system paralyzation.

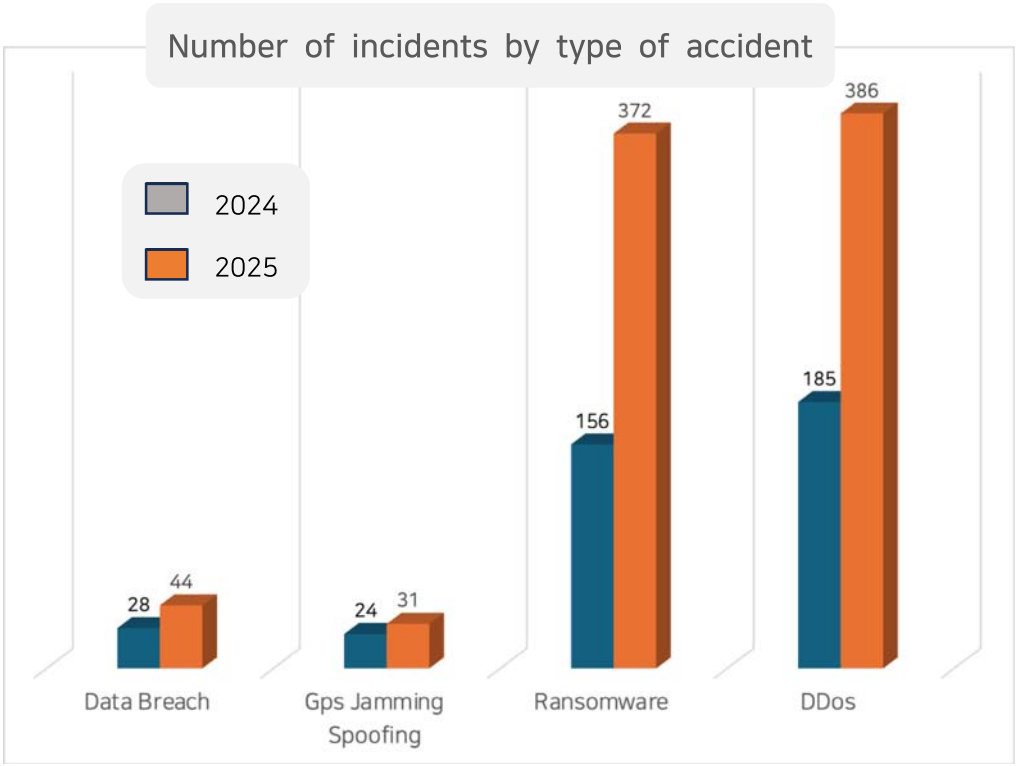
3. Full Compliance with Global Regulations

Our solutions provide the most effective way to demonstrate the threat monitoring and response capabilities required by the latest international maritime security standards, including IMO MSC-FAL.1/Circ.3 and IACS UR E26/E27.

Maritime Cyber Threat Overview

Compared to 2024, the number of maritime cyber incidents in 2025 has surged by 103%, emerging as a critical threat to maritime safety. Distributed Denial of Service (DDoS), Ransomware, and Malware infections account for the majority of these attacks, with their growth rate more than doubling over the past year.





Characteristics of Maritime Cyber Threat Types

1. Ransomware and Malware Infections

- Attack Vectors:
  Threats propagate into internal networks through attachments in phishing emails sent to crew members, insecure onboard public Wi-Fi, and the use of unverified USB flash drives.
- Characteristics:
  These attacks encrypt data within Planned Maintenance Systems (PMS), effectively holding voyage records hostage to demand ransom payments.

2. Distributed Denial of Service (DDoS)

- Attack Vectors: Attackers recruit IoT devices with weak security settings or onboard communication terminals into a botnet. They then paralyze systems by flooding satellite communication bandwidth with indiscriminate traffic at a specific time.

- Characteristics: By cutting off the connection with onshore Mission Control Centers (MCC), these attacks cause isolated vessels to lose their crisis response capabilities. Furthermore, hacktivist groups, such as NoName057(16), continue to launch persistent attacks targeting ports and government agencies.

3. GPS Spoofing and Jamming

- Attack Vectors: Attackers deceive antenna receivers by either emitting powerful radio interference signals (Jamming) or transmitting false signals that are stronger than actual satellite signals (Spoofing).

- Characteristics: By displaying fraudulent location data on navigation equipment —such as ECDIS (Electronic Chart Display and Information System) and AIS (Automatic Identification System)—attackers intentionally divert vessels from their intended routes or lure them into violating territorial waters.

4. Data Breach and Information Theft

- Attack Vectors: Attackers exploit vulnerabilities in maritime cloud services or remote maintenance channels connected to onshore networks to exfiltrate confidential information stored on servers.

- Characteristics: Sensitive data—including ship design schematics, voyage logs, cargo manifests, and crew personal information—is stolen to be sold on the Dark Web or leveraged as a foundation for more sophisticated secondary attacks.

5. OT (Operational Technology) System Intrusion and Loss of Control

- Attack Vectors: Attackers exploit the blurred security boundaries within integrated IT-OT networks to gain entry. Once inside, they can issue direct commands to critical control devices such as Integrated Automation Systems (IAS) and Ballast Water Management Systems (BWMS). There is also a rising trend of targeted attacks against maritime communication systems (VSAT) and navigation systems (ECDIS).

- Characteristics: By gaining forced control over the ship's physical movements, attackers can directly trigger catastrophic incidents, including collisions, groundings, and environmental disasters.

Regional Dynamics of Maritime Cyber Threats

Maritime cyber threats manifest in diverse ways across different regions, driven by varying geopolitical interests and economic values associated with each maritime zone. In conflict-prone areas such as the Strait of Hormuz and the Baltic Sea, system disruption activities—including GPS manipulation and electronic jamming—are prevalent, often orchestrated to achieve state-level military or political objectives.

In contrast, Asian waters and global hub ports with high shipping volumes frequently see data breaches and ransomware attacks by criminal organizations seeking to maximize financial gain.

Consequently, maritime cyber threats have evolved beyond simple technical hacking into complex, multi-faceted operations that reflect the unique regional characteristics and strategic tensions of the sea.

1. The Middle East – Strait of Hormuz and the Persian Gulf

Geopolitical tensions in this region remain exceptionally high. Recently, there has been a frequent discovery of GPS spoofing tactics used against oil tankers. These attacks manipulate the vessel's systems to show the ship as being within a specific country's territorial waters, even when it is actually navigating in international waters.

Such tactics are strategically employed to create a pretext for forcibly halting or seizing the vessel.

2. Asia – Strait of Malacca and the South China Sea

As a global hub for maritime trade, this region is increasingly targeted by "Cyber Pirates." Unlike traditional pirates who launched indiscriminate attacks, modern perpetrators now hack into shipping company networks to conduct

reconnaissance. By identifying which vessels are carrying high-value cargo and determining the exact number of onboard security personnel, they select and strike their targets with surgical precision.

3. Europe – Baltic Sea and the Black Sea Coast

Driven by the impact of the Russia-Ukraine war and other regional conflicts, widespread electronic interference has become a daily occurrence in this area. Commercial vessels passing through these waters frequently experience sudden GPS outages or find their location data displaced by hundreds of kilometers. These disruptions have become a direct cause of maritime accidents.

4. Global Major Hub Ports – Rotterdam, Los Angeles, Busan, etc.

Large-scale port terminals are prime targets for Ransomware. Attackers encrypt Terminal Operating Systems (TOS) to completely halt container loading and unloading operations, subsequently demanding exorbitant ransoms. This is because the paralyzation of even a single major port can trigger a severe bottleneck effect across the entire global supply chain.

Vulnerability Assessment of Onboard Maritime Equipment

Analysis of Cyber Threats by Maritime Equipment Type

Cyber threats targeting maritime equipment manifest in various forms—such as risks to navigation safety, vessel control, and cargo management—depending on the specific function of the equipment involved.

Therefore, to ensure the safe operation of a vessel, it is essential to understand the unique vulnerabilities of each piece of equipment where IT and OT systems converge. Based on this understanding, establishing a differentiated security response framework tailored to each system is a critical requirement.

1. Navigation & Communication Systems

These are critical components that can directly trigger physical maritime disasters, such as collisions and groundings.

(1) GNSS/GPS Receivers

- Threat Characteristics: Highly vulnerable to Spoofing (sending fake signals to cause location errors) and Jamming (blocking signals entirely).
- Incident Impact: Causes vessels to deviate from planned routes or unauthorized entry into neighboring territorial waters, leading to seizure or diplomatic disputes.

(2) AIS (Automatic Identification System)

- Threat Characteristics: Since it uses unencrypted, open wireless communication, attackers can manipulate data to create "Ghost Ships" or mask the signals of actual vessels.
- Incident Impact: Leads to interference with vessel tracking and causes critical errors in collision avoidance systems.

(3) ECDIS (Electronic Chart Display and Information System)

- Threat Characteristics: Highly susceptible to malware infiltration during software or chart updates via external media, such as USB drives.

- Incident Impact: If chart data is tampered with, the crew may fail to recognize hazards like submerged rocks, leading directly to grounding accidents.

2. Engineering Control & Automation Systems

These systems serve as the "heart" and "limbs" of the vessel; the primary objective of an attack here is the direct cessation of operations.

(1) Engine & Propulsion Control Systems

- Threat Characteristics: Communication channels intended for Remote Access (used for maintenance) are often exploited as entry points for hackers.
- Incident Impact: By manipulating engine output or forcing a system shutdown, attackers can render a vessel uncommandable. This poses a severe risk of collisions, especially within crowded port areas.

(2) Ballast Water Management Systems (BWMS)

- Threat Characteristics: Attackers target and manipulate the automated valve control logic to induce abnormal operations.
- Incident Impact: Compromising the ship's stability can lead to a risk of capsizing or result in environmental disasters due to improper ballast discharge.

3. Cargo Management & Network Systems

Attacks in this category are primarily linked to economic disputes or piracy-related activities.

(1) Loading Computers & Cargo Management Systems

- Threat Characteristics: These systems are vulnerable to attacks involving the tampering of invoices or the manipulation of cargo stowage data.
- Incident Impact: Loading errors involving hazardous materials can lead to explosion risks. Additionally, these systems can serve as a leak point, exposing information about high-value cargo to pirates.

(2) Onboard Public Networks & IoT Sensors

- Threat Characteristics: Highly susceptible to ransomware infections through BYOD (Bring Your Own Device) connections. Furthermore, low-cost IoT sensors with weak security often act as entry points for penetrating the entire onboard network.
- Incident Impact: These vulnerabilities can lead to total system paralysis, resulting in operational delays and significant recovery costs.

Maritime Industry Attack Types

Evolution of Cyber Attacks in the Maritime Industry

Cyberattacks on the maritime industry are unfolding along two primary axes: direct attacks aimed at seizing physical control of vessels and supply chain attacks designed to paralyze the broader maritime ecosystem.

In particular, as the digitization of ships increases the integration points between satellite communications and OT (Operational Technology) systems, attack patterns that were previously limited to simple data theft are now evolving into destructive forms that disrupt actual navigation or trigger catastrophic physical incidents.

1. Cyber Attacks Targeting Vessels

(1) Vulnerabilities in Satellite Communication (VSAT) Systems

The attack on Iranian vessels by Lab Dookhtegan in 2025 clearly demonstrated this risk. In two separate waves in March and August, the communications of approximately 180 vessels were paralyzed.

The attackers exploited weak credential management and outdated firmware to infiltrate the systems. After penetrating through the supply chain, the attackers destroyed system components, completely severing the link between the ships and onshore facilities and demonstrating a devastating capacity to neutralize onboard networks.

(2) GPS/GNSS Spoofing Attacks

The danger of spoofing was vividly illustrated by the grounding of the MSC Antonia in the Red Sea in May 2025. In this region, threats have become a daily reality, with over 1,000 vessels per day now affected by signal interference.

By exploiting the lack of authentication in GPS signals, attackers transmit counterfeit signals to distort navigation equipment and AIS location data. This

tactic intentionally diverts vessels from their intended routes, leading to physical collisions or groundings.

(3) Direct Attacks on OT (Operational Technology) Systems

A representative case is the RAT (Remote Access Trojan) installation discovered on the ferry Fantastic in December 2025. This incident occurred when a crew member, acting on external instructions, inserted a malware-laden USB drive directly into a bridge workstation. By exploiting vulnerabilities such as outdated operating systems (e.g., Windows XP) and inadequate network segmentation, this type of attack is considered the most lethal; it can manipulate ECDIS chart data to provide false information or remotely take over key engineering systems, resulting in a total loss of vessel control.

2. Supply Chain Attacks

(1) Targeting Shipyards and Maritime Equipment Manufacturers

A representative example is the theft of core design secrets perpetrated by groups such as North Korean APT groups or RansomHub. These attackers first compromise relatively vulnerable subcontractors to pivot into the main shipyard networks. Their objectives include stealing blueprints for warships and specialized vessels or encrypting production lines to delay construction schedules. Beyond mere financial loss, these actions lead to severe consequences, such as exposing vulnerabilities in national naval power and weakening the competitiveness of strategic national assets.

(2) Attacks on Terminal Operating Systems (TOS)

The risk has been proven through large-scale ransomware infections at major hub ports across Europe and North America. When hacktivists or criminal organizations paralyze cargo handling systems and logistics data, container operations grind to a halt, forcing tankers and cargo ships in nearby waters to wait indefinitely. Such attacks transcend the damage of a single port, triggering bottlenecks in the global supply chain and causing immediate chaos in the global economy, including spikes in oil prices and inflation.

(3) Attacks via Software and Communication Service Providers

These attacks unfold by planting malware into update servers or management tools. This method has the highest impact because a single breach can simultaneously distribute malicious code to tens of thousands of vessels worldwide that utilize the compromised software. Ironically, as autonomous navigation and remote maintenance technologies advance, these "trusted" update pathways have become the most dangerous attack vectors, causing a chain reaction of damage across numerous organizations and vessels.

Case Studies: Attacks on Vessels

The attack by Lab Dookhteganin 2025 serves as a prime example of the critical vulnerabilities inherent in maritime satellite communication (VSAT) systems and the global supply chain. This incident demonstrated a highly sophisticated Advanced Persistent Threat (APT) pattern, where political circumstances were strategically combined with cyber operations to systematically paralyze the maritime logistics network of a specific nation.

File photo of Iranian oil tanker 'Iran Ocean' operated
By the National Iranian Tanker Company (NITC)

Phase 1: Real-time Communication Shutdown via VSAT Infiltration(March 2025)

- **Impact Scale and Targets:**

  A total of 116 vessels were hit simultaneously, including 50 tankers from the National Iranian Tanker Company (NITC) and 66 ships from the Islamic Republic of Iran Shipping Lines (IRISL).

- **Perpetrator and Geopolitical Context:**

  The hacking group 'Lab Dookhtegan,' suspected of being linked to Israel, claimed responsibility, stating the attack aimed to "curb Iran's maritime terrorism and smuggling activities." The operation was strategically timed during peak regional military tensions, coinciding with U.S. airstrikes against Houthi rebels.

- Technical Attack Vector (The Falcon Breach):
  The attackers targeted vulnerabilities in 'Falcon,' a specialized software used for managing maritime satellite communications. By hijacking administrative privileges, the perpetrators were able to simultaneously alter or destroy the communication configurations of 116 vessels scattered across the globe.

- Detailed Impact:
  - Communication Blackout: All email, voice calls, and data transmissions between the vessels and onshore control centers were completely severed.
  - Loss of Tracking: Real-time vessel tracking systems were paralyzed, leaving operators in a high-risk situation where they could not determine the location of their national fleet.
  - Operational Delays: Since mandatory pre-arrival communications with ports became impossible, vessels were forced to wait indefinitely in nearby waters, causing massive logistical disruptions.

- Key Takeaway:
  This incident serves as a global warning to the maritime industry regarding the 'Single Point of Failure' risk, where a vulnerability in a single software platform can instantaneously paralyze the operations of an entire national fleet.

Phase 2: Large-scale Fleet Sabotage via Supply Chain Infrastructure Compromise (August 2025)

The second wave of attacks revealed the true nature of the operation, which remained partially obscured during the first phase. The core of this attack was not a simple modem-level hack; rather, it involved the direct infiltration of the data centers and hub infrastructure of 'Fanava Group,' Iran's primary IT and telecommunications holding company.

- Impact Scale and Targets:
  Continuing from Phase 1, a total of 64 vessels—including 39 NITC tankers and 25 IRISL cargo ships—were targeted for direct sabotage.

- Attack Vector (Provider-level Compromise):

  The attackers infiltrated the central infrastructure of the satellite service provider, Fanava, and remained latent for approximately five months to conduct reconnaissance. This allowed them to gain Root privileges at the central hub, granting them simultaneous access to the systems of dozens of vessels without needing to access each ship individually.

- Detailed Impact and Destructive Tactics:

  - Data Erasure (Sabotage): In the Linux-based vessel terminal systems, attackers used the 'dd' command to forcibly wipe six storage partitions. This caused catastrophic damage that transcended simple system failure, requiring the physical replacement of hardware.
  - Falcon Process Termination: By neutralizing 'Falcon,' the core software for maritime communication, they severed all ship-to-shore connectivity, including VOIP and data transmissions.
  - Exfiltration of Confidential Data: Internal network diagrams, operational checklists, and fleet management documents were stolen and leaked. Notably, by seizing real-time AIS tracking data around the Port of Bandar Abbas, the attackers monitored the entire movement of the Iranian fleet.

- Key Takeaway:

  This operation was not merely an act of espionage; it was a clear case of 'Sabotage' intended to paralyze a national logistics network. It proved that when a service provider becomes a 'Single Point of Failure,' an entire national fleet can be neutralized instantaneously

Case Studies: Attacks on Onboard Equipment

FURUNO Electric Ransomware Infection (2025)

In October 2025, FURUNO Electric, a premier global manufacturer of maritime electronic equipment, fell victim to a ransomware attack. This incident demonstrated that even without direct hacking of individual vessels, targeting the original equipment manufacturer (OEM) can cause widespread instability throughout global maritime safety infrastructure.

- **Impact Scale and Targets:**
  The attack struck the Japanese headquarters and global network systems of FURUNO, which produces critical navigation components such as Radar, ECDIS (Electronic Chart Display and Information System), and VDR (Voyage Data Recorder).

- **Perpetrator:**
  The attack was attributed to 'Rhysida,' an emerging ransomware group known for targeting government agencies and critical manufacturing infrastructure.

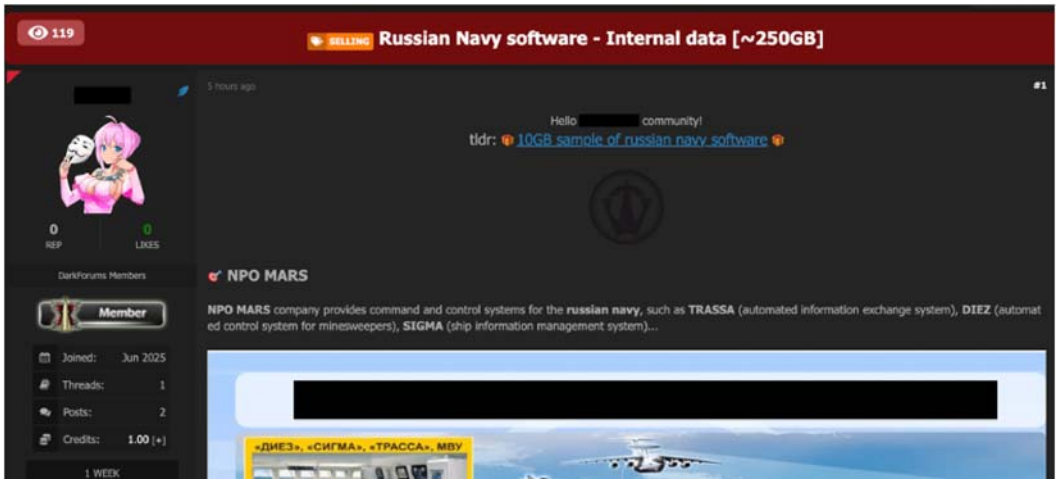
- **Attack Method (Double Extortion):**
  - Dual-track Pressure: The group employed a Double Extortion strategy—paralyzing operations by encrypting internal data while simultaneously threatening to leak sensitive exfiltrated data on the Dark Web.
  - Disabling Backups: This classic yet lethal tactic involved neutralizing the company's backup systems to prevent recovery and maximize the pressure to pay the ransom.

- **Detailed Impact and Consequences:**
  - Supply Chain Threat: FURUNO equipment is installed on a vast number of vessels worldwide. The paralysis of the manufacturer's systems led to the suspension of equipment maintenance, emergency software updates, and the supply of new parts, creating a safety vacuum for global fleets.

- Risk of Design Data Leakage: The gravity of the situation is heightened by the concern that if stolen data includes engineering blueprints or source code, it could serve as a foundation for future Zero-day attacks against ships currently utilizing those specific devices.

Case Studies: Attacks on Onboard Equipment

Data Breach at NPO Mars Defense Contractor (2025)



Attackers' post on a data leak forum. Image by Cybernews.

In July 2025, internal data from NPO Mars, a critical defense contractor responsible for developing the Russian Navy's combat command systems, was leaked on the Dark Web. This incident highlights the catastrophic security implications that arise when the blueprints of a vessel's "brain"—its Command and Control (C2) systems—are compromised.

- **Impact Scale and Targets:**
  Approximately 250GB of classified data was exfiltrated from the servers of NPO Mars, the primary designer of automated command and control systems for the Russian Navy.

- **Perpetrator:**
  While the specific identity of the threat actor remains unconfirmed, the breach became public when the stolen data was leaked on various Dark Web forums.

- **Detailed Impact and Leaked Assets:**
  SIGMA Combat Information System: Data regarding 'SIGMA,' the core command

and control framework for Russian naval vessels, was exposed. This means the logic governing armament operations and tactical decision-making is now potentially accessible to adversarial forces.

- DIEZ Minesweeper Control System: Technical information concerning automated control systems for minesweeping vessels (designed to detect and remove naval mines) was included in the leak.
- Technical Manuals and Blueprints: Detailed manuals covering system operational principles, network architectures, and hardware specifications were compromised, providing a foundation for adversaries to analyze and exploit system vulnerabilities.

- Strategic Impact:
  - Neutralization of Command and Control: With the exposure of tactical network structures, Russian naval communications are now highly vulnerable to Electronic Warfare (EW), including eavesdropping or the insertion of fraudulent commands during active engagements.
  - Loss of Asymmetric Advantage: The leakage of minesweeping system data allows adversaries to predict and counter Russian naval responses during mine-based blockade operations, posing a severe threat to maritime sea control.

Case Studies: Attacks on Shipyards

Data Breach at Sevmash Shipyard and Nuclear Submarine Secrets (2025)

Diagram of Russian submarine posted by HUR.

In August 2025, Sevmash Shipyard, one of Russia's most critical military installations, was targeted by a cyberattack from the Main Directorate of Intelligence of Ukraine (HUR). This incident had immense military repercussions as it specifically targeted core information regarding the 'Knyaz Pozharsky,' a state-of-the-art Borei-A class nuclear-powered ballistic missile submarine.

- **Impact Scale and Targets:**
  Servers at the Sevmash Shipyard in Severodvinsk, Northern Russia, were compromised, resulting in the exfiltration of a vast trove of classified data related to nuclear submarines currently under construction.

- **Perpetrator:**
  The operation was confirmed to have been carried out by cyber units under the Ukrainian HUR, conducted with the objective of neutralizing an adversary's key strategic assets during wartime.

- Detailed Impact and Leaked Information:
  - **Exposure of Physical Vulnerabilities:**
    Blueprints of the submarine's watertight compartments and technical vulnerability assessments were leaked. This essentially handed over "achilles' heel" information to the adversary, detailing exactly which sections to target to sink the vessel.
  - **Personnel Data Compromise:**
    Extremely sensitive personal information of 66 crew members was stolen, including names, ranks, physical fitness scores, and medical evaluations. This data could be exploited for targeted recruitment, blackmail, or psychological warfare.
  - Operational Secrets: Complete sets of combat manuals, operational schedules, and engineering blueprints were exfiltrated, allowing the adversary to predict the submarine's operational capabilities and transit patterns.

- Strategic Impact:
  - **Weakening of Nuclear Deterrence:**
    As the Borei-A class is a cornerstone of Russia's nuclear triad, the breach has cast significant doubt and uncertainty over Russia's maritime nuclear second-strike capabilities.
  - **Psychological Blow:**
    The fact that a top-tier national security facility—a nuclear submarine shipyard—was penetrated dealt a fatal blow to internal military morale and the perceived reliability of their security systems.

Case Studies: Attacks on Ports and Terminals

Ransomware Infection at Terport Terminal, Paraguay (2025)

In December 2025, Terport, a major terminal operator in Paraguay, fell victim to a ransomware attack. Because a Terminal Operating System (TOS) is critical infrastructure managing vessel arrivals/departures and container loading/unloading, attacks holding these systems hostage aim to maximize financial extortion.

- **Impact Scale and Targets:**
  The operational databases and management networks of Terport terminals, which serve as Paraguay's logistical lifelines, were compromised.

- **Perpetrator:**
  The attack was attributed to 'LYNX,' an emerging cybercrime group known for targeting large-scale logistics and manufacturing infrastructure to demand high ransoms.

- **Attack Method (Data Exfiltration & Ransom):**
  - Infiltration and Theft: The attackers penetrated the operational network to exfiltrate internal data before encrypting the entire system.
  - Double Extortion: They employed a classic double-extortion tactic, demanding payment not only for data recovery but also to prevent the public release of sensitive stolen information.
- **Detailed Impact:**
  - Logistics Records & Operational Data: Essential real-time data for port operations—including vessel schedules, cargo manifests, and container location data—were both leaked and encrypted.
  - Partner and Customer Information: Sensitive business data belonging to shipping lines, cargo owners, and logistics partners was compromised, raising concerns over secondary damages.

- Strategic Impact (Logistics Disruption):
  - Stoppage of Cargo Handling: System paralysis forced a shift to manual operations, drastically slowing container processing speeds and causing severe port congestion.
  - Erosion of Supply Chain Trust: The exposure of security vulnerabilities at a national logistics hub negatively impacted the confidence of global shipping lines regarding the terminal as a reliable port of call.

Case Studies: Attacks on Ports and Terminals

Paralysis of the Port of Antwerp-Bruges, Belgium (2025)

In the first half of 2025, the Port of Antwerp-Bruges—the second-largest port in Europe—faced an intensive cyberattack by nation-state-sponsored hacker groups. This incident clearly demonstrated how a port can become a strategic target during geopolitical conflicts, transcending mere financial motives.

- **Timeline:** First half of 2025

- **Perpetrators:**
  APT28 (Fancy Bear), a Russian-linked nation-state-sponsored group, and affiliated hacktivist organizations.

- **Targets:**
  The Terminal Operating System (TOS) and associated logistics networks of the Port of Antwerp-Bruges.

- **Attack Vectors:** DDoS and System Infiltration
  - Traffic Overload: Attackers launched a massive Distributed Denial of Service (DDoS) attack against the Terminal Operating System (TOS), the core of port operations, to paralyze it.
  - Infiltration: Simultaneously, they penetrated internal networks to exfiltrate logistics data and operational secrets in a complex, multi-vector attack.

- **Detailed Impact:**
  - Operational Stoppage: Systems for vessel arrival/departure management and container discharge scheduling were temporarily suspended.
  - Logistical Congestion: As automated handling equipment and gate systems became unresponsive, a massive logistical crisis ensued, with thousands of trucks and dozens of vessels stranded in nearby areas.

- Strategic Disruption:
  - Supply Chain Neutralization: The blockage of a critical gateway for energy and goods in Europe caused a chain reaction of disruptions in the industrial production of neighboring countries.
  - Geopolitical Pressure: Interpreted as a retaliatory strike against Western nations supporting Ukraine, this incident proved that cyberattacks can serve as a powerful asymmetric weapon, holding maritime logistics hostage.

Maritime Cyber Risk Outlook for 2026

[AI Sabotage] Entrenchment of AI Agent-Based Autonomous Attacks

2026 will mark the era of "Autonomous Attacks," where AI evolves beyond a supportive tool to independently execute operations. As demonstrated by the 2025 case of the China-linked group GTG-1002, AI agents can now perform up to 90% of the attack lifecycle—from vulnerability analysis to data exfiltration—without human intervention. This lowers the barrier to entry, enabling low-skilled threat actors to launch nation-state-level sophisticated attacks at scale, leading to an explosive increase in attack frequency against maritime organizations.

[Supply Chain Pivot] Dominance of High-Node Compromise and Chain Infections

Instead of targeting individual vessels, attackers will focus on "choke points" in the supply chain, such as telecommunication providers and OEM equipment manufacturers. The tactic of paralyzing an entire fleet by infiltrating a single satellite provider—as seen in the Lab Dookhtegan case—will become commonplace. In particular, attempts to exploit remote access vulnerabilities in certain maritime equipment will intensify. This suggests that the maintenance channels of equipment providers will serve as "Pivot" points to simultaneously infect multiple vessels.

[C2 Manipulation] Convergence of Command & Control (C2) Manipulation and Physical Strikes

"Cyber-Physical Attacks," where digital breaches lead to physical destruction, will become increasingly sophisticated. GPS jamming and spoofing in conflict zones will become a daily reality. Critically, hacker groups are expected to seize maritime C2 systems or AIS data to coordinate coordinates for actual missile strikes. This elevates cybersecurity from a technical issue to a matter of physical security, directly impacting the lives of seafarers and the survivability of vessels.

[Ransomware Cartel] Alliance between Hacktivism and Ransomware Syndicates

The "cartelization" of politically motivated hacktivists and profit-driven ransomware organizations will deepen. Mirroring trends seen in regional conflicts, hacktivists may rent Ransomware-as-a-Service (RaaS) infrastructure to indiscriminately strike an adversary's ports or logistics systems. These cartels will likely normalize double and triple extortion tactics and precisely target backup systems, focusing on high-value attacks with ransom demands averaging millions of dollars.

[Regulatory Pressure] Heightened International Security Regulations and Operational Risks

In 2026, regulatory compliance will become a critical risk factor determining the survival of maritime enterprises. As stringent requirements like IACS UR E26/27 become fully operational, vessels or equipment manufacturers failing to meet security certifications will face real operational risks, including loss of sailing credentials or denial of port entry. Furthermore, as "Shadow Fleets" remain blind spots for security vulnerabilities, international pressure and cyber sanctions to block these entities will intensify.

Strategic Response and Mitigation Measures

Building Proactive Security via Maritime Cyber Threat Intelligence (MCTI)

Organizations must transition from reactive defense to an active posture powered by Maritime Cyber Threat Intelligence (MCTI). The core of this strategy lies in the real-time collection and analysis of data regarding global GPS spoofing, ransomware targeting specific fleets, and VSAT vulnerabilities. By sharing this intelligence with Maritime Security Operations Centers (SOCs), vessels can perform "preventative defense"—applying critical patches before an attack occurs or heightening surveillance when entering high-risk waters, effectively eliminating information blind spots.

Threat Modeling-Based Prediction and Improvement for New and Existing Ships

A structured framework is required to apply Threat Modeling throughout the entire lifecycle of a vessel, from design to decommissioning. After clearly identifying onboard OT and IT assets, virtual simulations of data flows and attack vectors must be conducted. For high-risk assets with multiple external touchpoints—such as autonomous navigation systems and remote maintenance channels—potential attack scenarios should be predefined. These insights must lead to immediate design modifications or network isolation to preemptively neutralize risks.

Regularizing Security Testing for the Global Fleet

To maintain robust security post-deployment, regular security testing mimicking real-world infiltration scenarios is essential. For newbuildings, mandatory penetration testing prior to delivery should verify initial security integrity. For vessels in service, vulnerability scanning and satellite communication security audits must be conducted at least once a year. It is crucial to include practical tests that address human factors, such as crew errors or the use of unauthorized external storage, to ensure constant resilience against evolving attack techniques.

Establishing Cyber Security Management Systems (CSMS) for Shipping Lines and Shipyards

Beyond technical defenses, it is vital to establish a Cyber Security Management System (CSMS) to govern corporate-wide security. Based on international standards like ISO/IEC 27001 or the NIST Framework, maritime-specialized security processes must be developed. Shipyards should prioritize protecting core engineering blueprints and securing OT within production lines, while shipping lines must implement management systems covering fleet-wide remote monitoring and incident response protocols to secure the high level of trust demanded by the global market.

Strengthening Supply Chain Security and CSMS for Marine Equipment

Every piece of software and hardware installed on a vessel must be supplied in a security-verified state. Equipment manufacturers must embed security into the entire product development lifecycle and provide a Software Bill of Materials (SBOM) to enable immediate identification and remediation of vulnerabilities. By standardizing equipment security features in compliance with IACS UR E27, manufacturers can fundamentally block vulnerabilities at the lower tiers of the supply chain from escalating into threats for the entire vessel.

The Journey Toward Cyber Trust and Resilience: From Compliance to Verification

Strategic Insight: *2026, The Year of Practical Verification*

Data indicating a 103% surge in maritime cyber incidents in 2025 sends a clear warning: the era of disconnected seas is over. As Operational Technology (OT) systems integrate with satellite networks, the attack surface has expanded to unprecedented levels. As witnessed in the 2025 satellite infrastructure sabotage, a single breach can now expose national strategic assets and paralyze global supply chains.

Yet, 2026 signifies more than just rising threats. It marks a critical transition from "Paper Compliance" to "Practical Verification." Vessels contracted after the enforcement of IACS UR E26/E27 (July 2024) are scheduled for sea trials and delivery this year. Cybersecurity is no longer just a checkbox on a design blueprint; it has become a fundamental "License to Sail" that determines whether a ship can be delivered and operated.

To survive in this new era where AI-driven attacks and supply chain vulnerabilities are the norm, the maritime industry must embrace three core transformations:

- **Maritime-Specific Intelligence:**
  We must move beyond generic CTI to Maritime Cyber Threat Intelligence (MCTI). This requires understanding the unique language of the sea—such as NMEA and AIS protocols—and proactively tracking threat signals targeting vessel assets on the Dark Web.

- **Secure by Design:**
  Security cannot be an afterthought. We must implement a Cyber Security Management System (CSMS) that applies threat modeling from the initial design phase, ensuring compliance with international regulations (IACS UR E26/E27) is embedded into the vessel's DNA.

[Conclusion]

- **Cyber Resilience:**
  Acknowledging that no defense is impenetrable, we must shift our focus to Resilience—the ability to anticipate, withstand, and rapidly recover from attacks. Shipyards, shipping lines, and equipment manufacturers must form a collaborative governance ecosystem, sharing SBOMs and incident data to ensure business continuity under any circumstance.

In a field where reliable information has been scarce, we hope this white paper serves as a milestone that transforms vague anxiety into actionable confidence.

CYTUR promises to remain a steadfast guardian, providing Cyber Trust and Resilience to a maritime industry facing the rough waves of digital transformation. We stand ready to navigate these challenges with specialized intelligence that truly speaks the language of the sea.

Key Maritime Cybersecurity Terms

The core technical and regulatory terms covered in this white paper are defined below to help readers easily understand the content.

- **OT (Operational Technology):**
  Technology used to control and monitor physical devices, such as Integrated Automation Systems (IAS) for engine control and Ballast Water Management Systems (BWMS).
- **MCTI (Maritime Cyber Threat Intelligence):**
  Maritime-specific threat intelligence provided by analyzing maritime protocols (NMEA, AIS, etc.) and attack tactics unique to the maritime industry.
- **GPS Spoofing/Jamming:**
  Attacks that involve transmitting false satellite signals to distort location information (Spoofing) or using strong interference to block signal reception (Jamming).
- **IACS UR E26/E27:**
  Unified Requirements established by the International Association of Classification Societies (IACS) to ensure the cyber resilience of ships (E26) and onboard systems and equipment (E27).
- **CSMS (Cyber Security Management System):**
  A systematic cybersecurity management system established to protect an organization's assets and systems.
- **VSAT (Very Small Aperture Terminal):**
  A satellite communication system used on ships, serving as a primary channel for data exchange with shore-based stations and onboard network connectivity.
- **ECDIS (Electronic Chart Display and Information System):**
  A navigation information system that displays digital charts instead of paper charts and provides integrated management of navigation data.
- **AIS (Automatic Identification System):**
  A device that automatically exchanges navigational information, such as position, course, and speed, with other vessels and shore-based control centers.

Cybersecurity Self-Assessment Checklist for Maritime Enterprises

This checklist can be utilized by managers at shipping companies, shipyards, and equipment manufacturers to assess their current security levels and establish effective response strategies.

Assessment Area	Checklist Items	Result (V)
Policy & Management	Do you maintain a Cyber Security Management System (CSMS) that complies with international maritime security standards (e.g., IMO, IACS)?	
Threat Monitoring	Do you have a system in place to collect and analyze Maritime Cyber Threat Intelligence (MCTI) in real-time?	
Asset & Design	Are you identifying potential attack paths through threat modeling for ship IT/OT assets?	
Supply Chain Security	Have you secured Software Bills of Materials (SBOM) for major equipment and verified the security of your suppliers?	
Incident Response	Do you have scenario-based emergency response procedures for situations such as VSAT disconnection or system paralysis?	
Regular Testing	Do you conduct security tests, such as penetration testing, on both newbuilds and existing vessels at least once a year?	
Personnel Security	Do you conduct regular training for crew members on security protocols, such as USB usage restrictions and phishing email response?	

CONTACT US

If you require more detailed information regarding the 2025 maritime cyber threat analysis and 2026 risk outlook covered in this white paper, or if you need technical consultation on establishing cybersecurity strategies across the maritime industry, please feel free to contact us through the channels below at any time.

CYTUR realizes the ‘Secure by Design’ philosophy throughout the entire lifecycle of a vessel—from design to operation—and is committed to being the optimal partner in protecting our clients' valuable maritime assets and ensuring business continuity.

CYTUR Inc. | Cyber Trust & Resilience for Maritime
E-mail: sales@cytur.net
Website: http://cytur.net