Maritime Cybersecurity News Digest

Period: 16.03–31.03.2026

Maritime Cyber Weekly — Free
Headline-level maritime cyber news, delivered weekly. Quick 3-minute scan.
Subscribe Free →

Maritime Cyber Intelligence Brief — Premium
This report — semi-monthly deep-dive with full analysis, regulatory tracking, and tabletop links.
Subscribe for full access →

Section 1: Incidents & Attacks

Intelligence note: The 16–31 March 2026 window yielded one confirmed new maritime cyber incident (Port of Vigo ransomware) alongside ongoing GNSS disruption from the Hormuz crisis and a cross-sector ICS threat campaign. Open-source reporting was dominated by the IMO FAL 50 regulatory milestone and conference outputs rather than new discrete attacks. This is flagged transparently per editorial policy — quality over volume.

[INCIDENT] 1. Ransomware encrypts cargo traffic management systems at Port of Vigo — The Record

[Regulatory: NIS2] [Asset: Port OT | Corporate IT]

[HIGH] In the early hours of 24.03.2026, at approximately 05:45 local time, ransomware struck the cargo traffic management servers at Spain's Port of Vigo — Europe's largest fishing port by volume. Port authorities immediately disconnected affected systems and reverted to manual and paper-based operations to maintain continuity. Physical cargo handling and vessel movements continued without interruption, preventing a full operational shutdown, but the incident exposed the fragility of digitally-dependent port logistics. As of 31.03.2026, no ransomware group had claimed responsibility, and investigators were still working to establish the intrusion vector and determine whether data exfiltration occurred alongside encryption.

What this means: The ability to fall back on manual operations prevented operational paralysis, but the incident underscores that port OT systems handling cargo scheduling and traffic management must be treated as critical infrastructure with offline fallback procedures and tested isolation protocols — not just corporate IT continuity plans.

Source: The Record (Recorded Future) | Date: 24.03.2026 | Credibility: High Additional sources: Security Boulevard, The Cyber Express, Integrity360

Test your response: Practice your port's ransomware response plan in our free tabletop exercise →

[GNSS] 2. Strait of Hormuz — 1100+ vessels hit by GPS/AIS disruption as GNSS interference surges 50% — Windward

[Regulatory: n/a] [Asset: PNT/GNSS | Shipboard OT | Satcom/VSAT]

[CRITICAL] Ongoing since late February 2026, the scale of GNSS disruption in the Strait of Hormuz and surrounding waters was confirmed by Marlink telemetry on 25.03.2026 to have surged over 50% during March. Windward analysis identified 21 new AIS jamming clusters across UAE, Qatar, Oman, and Iranian waters, bringing the total number of affected vessels above 1100. GPS signals are being jammed to confuse drone and missile targeting systems — with the ships caught in the crossfire. Position displays aboard affected vessels were recorded showing locations at airports, a nuclear power plant, and multiple inland sites. AIS transponder data has been corrupted at scale across the world's most critical oil transit chokepoint, carrying roughly 20% of global seaborne oil.

What this means: Operators routing vessels through the Strait of Hormuz must treat GNSS as an unreliable input and enforce mandatory cross-checking against radar, gyrocompass, and celestial fixes; VSAT antenna pointing systems that depend on GPS may also be degraded, potentially disrupting critical safety and commercial communications simultaneously.

Source: Windward | Date: 25.03.2026 | Credibility: High Additional sources: OCCRP, Smart Maritime Network, Splash247, Bloomberg

Test your response: Practice navigating a GPS spoofing crisis in our free tabletop exercise →

[THREAT] 3. Iran-linked campaign targets critical infrastructure ICS/OT; Cl0p exploits MFT systems used in port logistics — Unit42

[Regulatory: n/a] [Asset: Port OT | Shipboard OT | Supply Chain]

[**HIGH**] Palo Alto Networks Unit42 updated its Iran threat brief on 26.03.2026, reporting an active Iran-linked campaign targeting critical infrastructure OT environments. Directives issued to targeted organisations recommend immediate isolation of internet-facing PLCs and ICS/OT systems from corporate networks. Concurrently, Cl0p ransomware affiliates have been actively exploiting two Cleo Managed File Transfer vulnerabilities — CVE-2024-55956 and CVE-2024-50623 — with MFT systems widely used across maritime supply chains for port logistics data exchange, cargo documentation, and customs integration. The cross-sector campaign has direct relevance to port operators whose MFT infrastructure processes high-value commercial and regulatory data flows.

What this means: Port and shipping operators running Cleo MFT or similar file transfer infrastructure should apply patches for CVE-2024-55956 and CVE-2024-50623 as an emergency priority, and audit internet-facing PLC or SCADA exposure immediately given the confirmed targeting posture of Iranian threat actors toward critical infrastructure OT.

Source: Unit42 (Palo Alto Networks) | Date: 26.03.2026 | Credibility: High Additional sources: TechJack Solutions

---

Section 2: Regulations & Standards

[REGULATION] 4. IMO FAL 50 approves Maritime Cyber Code roadmap and mandatory MSW cybersecurity — DNV

[Regulatory: IMO MSC.428 | IMO MSC-FAL.1/Circ.3] [Asset: Corporate IT | Port OT | Shipboard OT]

The 50th session of the IMO Facilitation Committee (FAL 50), held 23–27.03.2026 in London, produced the most substantive maritime cybersecurity regulatory decisions since MSC.428(98). The Committee agreed to develop a goal-based, non-mandatory Maritime Cyber Code targeting 2028 completion, covering ships, ports, and the ship-to-shore interface. Separately, amendments to the FAL Convention introducing mandatory cybersecurity requirements for Maritime Single Window (MSW) systems were approved in principle, with adoption targeted at FAL 51 in 2027. An IMO Strategy on Maritime Digitalization was approved in principle, and a correspondence group was established to develop the Cyber Code roadmap. The decisions represent a significant step toward a consolidated international framework spanning the entire port-ship interface rather than ship-only requirements.

What this means: Port operators and shipping companies managing MSW integrations should begin aligning their cybersecurity architecture to emerging FAL Convention requirements now — the 2027 adoption timeline is short enough to affect procurement and system design decisions being made today.

Source: DNV | Date: 27.03.2026 | Credibility: High

Test your response: See how IMO cyber requirements play out during a Port State Control inspection →

[REPORT] 5. BIMCO Cyber Security Survey 2026 launched to benchmark industry risk posture — BIMCO

[Regulatory: BIMCO Guidelines] [Asset: Shipboard OT | Corporate IT]

BIMCO launched its Cyber Security Survey 2026 on 25.03.2026, inviting shipping companies, managers, and operators to submit data on cyber risk practices, incident experience, and defensive measures. The survey is designed to quantify how accelerating digitalization, AI adoption, and the deteriorating geopolitical threat environment are reshaping maritime cyber exposure across the sector. Results will directly inform future revisions to BIMCO cybersecurity guidelines — the de facto voluntary standard referenced by many insurers and Port State Control authorities. Participation is open to all maritime stakeholders through mid-2026.

What this means: Completing the survey gives shipping companies an opportunity to shape the next generation of BIMCO guidelines; the aggregate data will also provide the sector's first evidence-based picture of how AI-era threats are changing actual incident rates and defensive investment across fleet types.

Source: BIMCO | Date: 25.03.2026 | Credibility: High

[REPORT] 6. CYTUR releases sector-specific Maritime Cyber Threat Briefs and Standard Response Guide — Cyprus Shipping News

[Regulatory: IMO MSC.428 | IACS E26/E27] [Asset: Shipboard OT | Port OT | Supply Chain]

In late March 2026, CYTUR published tailored Maritime Cyber Threat Briefs for three distinct maritime sub-sectors: shipping lines, shipyards, and equipment OEMs. Each brief includes a 28-item self-diagnostic checklist grading security posture and delivering 30/90/180-day remediation roadmaps. Alongside the briefs, CYTUR released a Standard Response Guide structured as a 4-stage cycle: Secure by Design, Threat Intelligence, Scenario-based Playbooks, and Forensics/Reporting. The playbook library includes GPS spoofing response, OT ransomware containment, autonomous vessel AI attack scenarios, and VSAT disruption procedures. All materials cross-reference IMO MSC.428, IACS E26/E27, IEC 62443, and ISO 27001.

What this means: The sector-specific framing makes these guides immediately actionable for organisations that have struggled to apply generic cybersecurity frameworks to maritime OT contexts; the 30/90/180-day roadmap format is particularly useful for boards and executive teams needing a structured investment case.

Source: Cyprus Shipping News | Date: 30.03.2026 | Credibility: Medium Additional sources: Splash247

[REGULATION] 7. NIS2 transposition under pressure — EU ports and maritime operators facing July 2026 enforcement cliff — Critical Entities Resilience Directive Portal

[Regulatory: NIS2] [Asset: Port OT | Corporate IT]

A European Commission assessment circulated in mid-March 2026 confirmed that transposition of both the NIS2 Directive and the CER (Critical Entities Resilience) Directive remains highly uneven across member states. Many member states missed the initial October 2024 transposition deadline and are now racing to finalise national legislation before the strict July 2026 enforcement deadline. Maritime and port entities are caught in the transitional gap: they face the legal obligation to comply but in many jurisdictions have not yet been formally identified and designated as critical entities — a prerequisite for enforcement action. Once designation occurs, incident notification obligations, supply chain security requirements, and security measure mandates apply immediately.

What this means: Port operators and maritime companies with EU operations should not wait for formal designation — initiating NIS2-aligned gap assessments now ensures that when designation arrives, remediation is already underway rather than just beginning.

Source: Critical Entities Resilience Directive Portal | Date: mid-March 2026 | Credibility: Medium

Test your response: Test your NIS2 incident notification readiness in a ransomware scenario →

Section 3: OT/ICS Threats & GNSS/PNT

[OT] 8. GNSS interference blinds VSAT antenna systems — Marlink warns of cascading satcom failures on connected vessels — Smart Maritime Network

[Regulatory: n/a] [Asset: Satcom/VSAT | Shipboard OT | Corporate IT]

[**HIGH**] Beyond the navigational impact documented in the Hormuz reporting (Item 2), Marlink's 25.03.2026 advisory revealed a less obvious but operationally critical consequence: GNSS interference is degrading VSAT antenna acquisition and pointing systems that depend on GPS coordinates for satellite tracking. When antenna controllers receive spoofed or jammed position data, they lose lock on the target satellite, severing all onboard connectivity — remote fleet management, GMDSS-linked services, over-the-air software updates, and crew welfare communications. Marlink confirmed the effect extends across GPS, Galileo, GLONASS, and BeiDou signals simultaneously, meaning multi-constellation receivers offer no protection against broadband jamming. The company issued crew guidance covering power-cycling antenna controllers and manual position entry, and is deploying interference-resistant reception hardware and signal anomaly detection across its managed fleet.

What this means: Fleet managers should confirm with their satcom provider whether interference-resistant firmware and anomaly detection are active on all vessels transiting contested regions; crews should be briefed that satcom outages in these areas may have an electronic warfare origin rather than a hardware fault — standard troubleshooting (reboot, check cables) will not resolve the root cause.

Source: Smart Maritime Network | Date: 25.03.2026 | Credibility: Medium Additional sources: Industrial Cyber (26.03.2026), Hellenic Shipping News (27.03.2026)

[REPORT] 9. Waterfall Threat Report 2026: ransomware slowdown masks nation-state pivot toward OT infrastructure — Industrial Cyber

[Regulatory: n/a] [Asset: Shipboard OT | Port OT]

[**HIGH**] Released on 27.03.2026, the Waterfall Threat Report 2026 documents a decline in publicly reported OT/ICS breaches with physical consequences from 76 in 2024 to 57 in 2025 — but argues the headline figure conceals a strategic shift: nation-state and hacktivist attacks on OT infrastructure doubled year-on-year. Maritime-relevant cases cited include grounded and misdirected vessels resulting from GNSS interference and control-system outages at port infrastructure. The report advocates that vessel operators and port managers treat independent verification of external inputs — particularly GPS — and unidirectional ICS data diodes as core safety controls equivalent to mechanical safety systems, not optional cybersecurity enhancements.

What this means: The declining ransomware count should not be read as improvement in maritime OT security; the doubling of nation-state and hacktivist OT incidents represents a structurally more dangerous threat class, and organisations that have calibrated their defences to the ransomware threat model may be exposed to adversaries with fundamentally different objectives and capabilities.

Source: Industrial Cyber | Date: 27.03.2026 | Credibility: High

---

[GNSS] 10. RNT Foundation: LEO PNT alternatives catalogue grows to 14 projects as GNSS disruption drives market — RNT Foundation

[Regulatory: n/a] [Asset: PNT/GNSS]

On 29.03.2026, the RNT Foundation flagged an updated FrontierSI Global LEO PNT report cataloguing 14 Low-Earth-Orbit PNT projects, up from 9 previously documented. The growth is explicitly linked to escalating GNSS disruption globally, with maritime stakeholders among the primary demand drivers. The 14 projects span commercial and government programmes offering independent positioning and timing signals that operate outside the GPS, Galileo, GLONASS, and BeiDou constellations subject to jamming and spoofing. The report reflects a wider industry

shift toward multilayered resilient PNT architectures in which GNSS provides one input among several rather than functioning as sole-source navigation infrastructure.

What this means: Naval architects, fleet operators, and port infrastructure managers evaluating long-term navigation resilience strategies should incorporate LEO PNT as a near-term procurement option rather than a future technology — several of the 14 catalogued programmes are already in commercial service or approaching operational availability.

Source: RNT Foundation | Date: 29.03.2026 | Credibility: High

---

Section 5: People, Training & Governance

[GOVERNANCE] 11. MTS-ISAC Maritime Cyber Resilience Summit Europe — Athens — MTS-ISAC

[Regulatory: n/a] [Asset: Corporate IT | Port OT | Shipboard OT]

The MTS-ISAC Maritime Cyber Resilience Summit Europe convened on 16–17.03.2026 at the Grand Hyatt Athens, bringing together port authorities, terminal operators, shipping lines, regulators, insurers, and cyber vendors for the largest operator-focused maritime cyber gathering in the European calendar. The agenda covered the current maritime threat landscape, third-party and vendor ecosystem risk, AI integration in maritime operations, and a dedicated incident response block titled "Phish and Ships" drawing on insights from over 100 incidents compiled by NORMA Cyber. Discussions on SOC models, satellite communications risk, and structured information sharing between operators produced actionable recommendations that MTS-ISAC will incorporate into its member guidance.

What this means: The synthesis of 100+ real maritime incidents into a single actionable exercise format represents a step-change in the quality of sector-specific preparedness material available to operators; companies not yet participating in MTS-ISAC information sharing are forgoing structured access to anonymised incident intelligence that is directly applicable to their own threat models.

Source: MTS-ISAC | Date: 16.03.2026 | Credibility: High

[GOVERNANCE] 12. NORMA Cyber Spring Conference + Annual Threat Assessment — Oslo — NORMA Cyber

[Regulatory: n/a] [Asset: Shipboard OT | Port OT | Corporate IT]

NORMA Cyber's Spring Conference on 24.03.2026 (open) and Member Council on 25.03.2026 (closed, vendors excluded) drew over 140 stakeholders from Norwegian and international maritime organisations. The open conference launched the NORMA Annual Threat Assessment covering sector-specific incident patterns, vulnerability trends, and defensive measures for Norwegian maritime — including state-sponsored campaigns targeting Nordic shipping and energy infrastructure. The closed Member Council enabled classified incident sharing between operators, reinforcing NORMA's position as a trusted national information-sharing hub for the Norwegian maritime sector and a model for equivalent structures elsewhere.

What this means: The two-tier format — open assessment for broad awareness, closed council for classified sharing — illustrates the structural approach needed for effective maritime cyber information sharing; operators in other national markets lacking equivalent structures are at a disadvantage in understanding their actual threat environment.

Source: NORMA Cyber | Date: 24.03.2026 | Credibility: High

Section 6: Upcoming Maritime Cyber Events

This section lists upcoming conferences and events in the next six weeks (until mid-May 2026). Data from the Maritime Cybersecurity Conference Calendar.

CS4CA APAC 2026 | 01–02.04.2026 | Singapore Approximately 150 senior IT/OT security leaders from critical infrastructure sectors including maritime and ports. Industrial cyber resilience, OT incident response, cross-sector threat intelligence. Link

IRClass Maritime Cyber Risk Management Training | 10.04.2026 | Online Classification-society-backed training for shipowners, managers, and port/terminal operators. IMO and IACS E26/E27 aligned curriculum. Link

4th Annual Maritime Cyber Safety Summit | 13.04.2026 | Miami, USA Invitation-only summit co-hosted by Carnival, Royal Caribbean, and NCL. OT cybersecurity for cruise vessels and passenger ship operations. Co-located with Seatrade Cruise Global. Link

Smart Maritime Network Rotterdam | 15.04.2026 | Rotterdam, Netherlands Port Community Systems (PCS) security: a cyberattack on Rotterdam's PCS could freeze European supply chains; focused discussion on incident response for port digital infrastructure. Link

Navy League NYC Maritime Security Conference | 15.04.2026 | New York, USA Cybersecurity, supply chain resilience, and US maritime dominance. Federal and commercial maritime security stakeholders.

Singapore Maritime Week 2026 | 20–24.04.2026 | Singapore Asia's largest maritime event. Hosts the "Marine CyberSafe" forum and Maritime Cyber Assurance Operations Centre showcase alongside commercial and regulatory programming. Link

People Tech Maritime — Athens | 21–22.04.2026 | Athens, Greece Digitalisation for Greek shipowners: cloud migration security, satellite network protection, and crewing technology. Link

Black Hat Asia 2026 | 21–24.04.2026 | Singapore Technical information security with research tracks on Cyber-Physical Systems including documented hacks on ECDIS, AIS, and maritime embedded systems. Link

BIMCO Digitalisation & Cyber Risks Seminar | 11.05.2026 | Online Legal and risk seminar covering cyber threat types for OT and navigation systems, BIMCO Cyber Security Clause 2019, liability frameworks, and cyber insurance market developments. Link

RiskTech Marine 2026 | 13.05.2026 | London (Lloyd's Building) Cyber, climate, and regulatory pressures reshaping marine risk. Dedicated tracks on OT/IT cyber safety, vessel-port integration security, and AIS/GPS manipulation risk. Link

Recent Events — March 2026

MTS-ISAC Maritime Cyber Resilience Summit Europe | 16–17.03.2026 | Athens, Greece
Operator-driven summit: threat intelligence, SOC models, satellite communications risk, ~100+ incident case studies via *Phish & Ships* exercise block. Link

People Tech Maritime — Oslo | 17.03.2026 | Oslo, Norway
Human-machine interface, crew training, and the "human firewall" concept in vessel autonomy operations. Link

Baltic Security Conference | 19.03.2026 | Riga, Latvia
Largest Baltic security event: IT security, crisis management, physical security with maritime domain relevance. Link

South Coast Cyber Summit | 23.03.2026 | USA
Critical-infrastructure cyber summit with dedicated maritime cyber risk keynote & tabletop exercises, co-hosted by Maritime Cybersecurity Institute.

RSA Conference 2026 | 23–26.03.2026 | San Francisco, USA
Premier global cybersecurity event with transport and critical infrastructure tracks. Link

NORMA Cyber Conference | 24.03.2026 | Oslo, Norway
Annual Threat Assessment launch, 140+ stakeholders, state-sponsored maritime & energy threat briefings. Link

Port of the Future Conference | 24–26.03.2026 | Houston, USA
Port Infrastructure 4.0: cybersecurity, automation, and digital resilience across maritime domains. Link

APM 2026 (Asia Pacific Maritime) | 25–27.03.2026 | Singapore
Massive maritime expo with MarineTech and cyber floors showcasing the latest maritime cybersecurity solutions for the Asian market. Link

---

Report compiled: 01.04.2026 | Coverage period: 16.03–31.03.2026 | Sources: 28 unique sources across Tier 1–4