Maritime Cybersecurity News Digest

Period: 16.05–31.05.2026

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 16–31.05.2026 fortnight was markedly quieter for direct attacks than the early-May Strait of Hormuz spike covered in the previous brief, and was instead dominated by regulatory and advisory activity. The headline developments were IMO MSC 111 (13–22.05) adopting the non-mandatory MASS Code and endorsing the roadmap toward a future Maritime Cyber Code; two CISA ICS advisory batches (19.05 and 28.05), the latter including the rare model-specific advisory ICSA-26-148-01 on the MacGregor VDR-G4e shipboard voyage data recorder; Carnival Corporation's disclosure of a breach affecting nearly 6 million people (notifications from 27.05, though the underlying intrusion dated to April); and a westward intensification of Russia-linked GNSS jamming into the Finnish Archipelago Sea and the Sea of Åland (24–25.05). Targeted name-checks across the major container lines, cruise operators, named ports and classification societies surfaced no new in-window large-scale ransomware or wiper attack beyond the Carnival disclosure — consistent with a genuine lull rather than a reporting gap. Note also that several items circulating in late May as "current" in fact dated to earlier periods — the 14-state Baltic GNSS open letter (January 2026), the "+1100 vessels" Middle East Gulf jamming figure (March 2026), and the Inmarsat/ClassNK UR E26/E27 whitepaper (2024) — and were excluded on event-date grounds.

[INCIDENT] 1. Carnival Corporation discloses data breach affecting nearly 6 million — social-engineering intrusion claimed by ShinyHunters, notifications begin 27.05 — Help Net Security

[Regulatory: n/a] [Asset: Corporate IT]

[HIGH] On 27.05.2026 Carnival Corporation — the world's largest cruise operator (brands include Carnival Cruise Line, Princess, Holland America Line, Cunard and Costa) — began notifying nearly 6 million people (5 995 277 per the Maine Attorney General filing) that their personal data had been compromised. According to the breach notice, the intrusion began on 14.04.2026 when an employee was deceived through social engineering into granting network access; the attacker accessed and copied data through 22.04.2026 before being blocked. The data extortion group **ShinyHunters** is named as the threat actor and claimed roughly 8.7 million records and 7.5 million unique email addresses. The exposed data comprised full names, dates of birth, gender, email addresses, Mariner Society loyalty status and tier, and internal customer identifiers; Carnival states this incident did not involve passwords, payment-card data or government identifiers — distinguishing it from earlier Carnival breaches. The disclosure surfaced through US state Attorney General filings and breach-notification letters from 27–28.05.2026.

What this means: The in-window event here is the disclosure and notification phase — which starts US state breach-notification clocks and is already drawing class-action activity — rather than the April intrusion itself. The operational lesson for maritime CISOs is the vector: a single employee social-engineered into granting access, not malware, defeated the perimeter. Identity-proofing at the help desk, least-privilege, and step-up verification for access grants are the control surface. The gap between ShinyHunters' claim (8.7 million) and the notified figure (around 6 million) is also a reminder that leak-site numbers are negotiation leverage, not ground truth — anchor incident-comms on verified counts.

Source: Help Net Security | Date: 28.05.2026 | Credibility: High Additional sources: Reuters, Malwarebytes, SecurityAffairs

[GNSS] 2. Russia-linked GNSS jamming intensifies and spreads west in Finnish Baltic waters — Archipelago Sea and Sea of Åland now affected — Anadolu Agency

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

[HIGH] On 24–25.05.2026 Finland's West Finland Coast Guard District, through Deputy Commander Pekka Niittylä, publicly warned that GPS/GNSS interference has intensified and spread westward from the Gulf of Finland into the Archipelago Sea and the Sea of Åland, degrading satellite navigation for commercial shipping and ferries in some of the busiest, most constrained sea lanes in the Baltic. Officials attributed the jamming to Russian electronic-warfare systems — secondary reporting points to Murmansk-BN equipment deployed in Kaliningrad — and linked the activity to the protection of Russian Baltic ports recently targeted by Ukrainian strikes. Larger vessels with higher-mounted receivers are more affected than small craft. Mariners were advised to carry updated paper charts, maintain radar- and chart-based navigation, and prepare for prolonged GNSS outages; the standing Sjöfartsverket NAVTEX warnings for Baltic GNSS/AIS/radar interference remained in force throughout the period.

What this means: The operationally significant change is geographic, not just intensity: interference moving into the Archipelago Sea and Åland brings it into dense ferry and pilotage waters where loss of position compounds collision risk in confined channels. Baltic operators should treat GNSS denial as the planning baseline rather than the exception — pre-briefed dead-reckoning and radar-fixing procedures, ECDIS sensor-validation alarms, and crew drills for sudden position loss during pilotage. Every event should still be logged to NAVCEN and coastal authorities; under-reporting masks the true footprint of the interference network.

Test your response: Simulate a confined-waters transit where ECDIS, AIS and your ship's GNSS position can no longer be trusted →

Source: Anadolu Agency | Date: 25.05.2026 | Credibility: High Additional sources: Daily Sabah, Militarnyi

---

Section 2: Regulations & Standards

[REGULATION] 3. IMO MSC 111 adopts non-mandatory MASS Code and endorses roadmap toward a Maritime Cyber Code — DNV

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

The 111th session of the IMO Maritime Safety Committee (MSC 111) met in London on 13–22.05.2026. The Committee adopted the non-mandatory International Code of Safety for Maritime Autonomous Surface Ships (MASS Code) — a goal-based framework covering the safety, operation and security of remotely-controlled and autonomous ships, reported as effective from 1 July 2026 — with an experience-building phase leading toward a mandatory MASS Code targeted to enter into force on 1 January 2032. On cyber, MSC 111 endorsed the roadmap and work plan (including intersessional working groups) for developing a new, initially non-mandatory cybersecurity code for ships and port facilities, following the IMO Facilitation Committee's (FAL 50) approval of that work plan in March 2026. The existing Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) remain in force unchanged; the publicly available class-society summaries (ABS, Lloyd's Register, DNV, ClassNK) do not name individual sponsoring states for the cyber-code initiative.

What this means: This is the period's most consequential regulatory signal. The direction of travel is unambiguous — maritime cyber requirements are moving from high-level guidance toward a structured, eventually auditable code, in parallel with the MASS Code embedding security into autonomous-ship design. Shipowners, port authorities and class-driven suppliers should treat the roadmap endorsement as the opening of a multi-year compliance runway and align now with IACS UR E26/E27 and MSC-FAL.1/Circ.3 rather than waiting for a mandatory instrument. The non-mandatory MASS Code becoming effective 1 July 2026 also makes its security provisions a live design reference for any remotely-operated or autonomous tonnage on order.

Test your response: Rehearse a class/flag cyber inspection under the IMO cyber-risk framework before the auditor is on the gangway →

Source: DNV | Date: post-22.05.2026 | Credibility: High Additional sources: Lloyd's Register MSC 111 summary, ABS regulatory news, ClassNK MSC 111 summary (PDF), IMO MSC 111 preview

---

[REGULATION] 4. NIS2 enforcement pressure builds on ports and transport as mid-2026 focus shifts to reporting discipline and accountability — NIS2.news

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

Legal and compliance commentary published in late May 2026 underscores that, with the EU NIS2 Directive's October 2024 transposition deadline long passed, regulators across Member States are now shifting from "are you in scope" toward enforcement of incident-reporting discipline, forensic evidence preservation and management accountability — areas where seaports, terminal operators and maritime logistics hubs remain unevenly prepared. NIS2 places ports and water-transport operators among essential/important entities, with the Article 23 reporting cascade — a 24-hour early warning, a 72-hour incident notification and a one-month final report — and personal liability for senior management. This is regulatory context rather than a discrete event: no new maritime-specific NIS2 instrument was issued in the window, but the commentary reflects a genuine mid-2026 reality for European port and shipping entities.

What this means: Large EU ports and shipping lines should assume they are now firmly inside NIS2's enforcement perimeter. The practical, low-regret steps are unchanged but increasingly urgent: pre-built per-jurisdiction CSIRT contact and reporting playbooks (so the 24/72-hour clocks start cleanly), log retention and chain-of-custody procedures for OT incidents, and board-level sign-off that someone owns the obligation. Multinational operators should expect each in-scope national subsidiary to generate its own parallel reporting workstream.

Test your response: Run the NIS2 reporting clock end-to-end — what happens in the first 24 hours when a port entity is hit and the regulator is waiting →

Source: NIS2.news | Date: 30.05.2026 | Credibility: Medium Additional sources: ProofAnchor — NIS2 incident-evidence guide

---

Section 3: Threats — OT/ICS and GNSS/PNT

[VULNERABILITY] 5. CISA advisory flags admin-takeover risk on the MacGregor VDR-G4e shipboard voyage data recorder (ICSA-26-148-01) — JVN / JPCERT VU#92172885

[Regulatory: USCG MTS Rule | n/a] [Asset: Shipboard OT]

[HIGH] On 28.05.2026 CISA published ICS advisory ICSA-26-148-01 covering the MacGregor Voyage Data Recorder (VDR) G4e — built by Danelec, the maritime equivalent of an aircraft "black box," continuously recording bridge audio, radar, ECDIS, AIS and sensor data aboard commercial vessels and mandated as safety equipment under SOLAS. The advisory was the first of nine new ICS advisories CISA released that day; the same batch covered a PUSR USR-W610 serial-to-Wi-Fi/Ethernet converter (a device class common in maritime and industrial OT telemetry), ABB EIBPORT and Busch-Welcome door controllers, CP Plus and KMW CCTV/network video recorders, Schneider EcoStruxure Machine Expert HVAC, and the XCharge C6. The advisory documents five vulnerabilities in VDR-G4e firmware prior to V5.250 — the two most serious rated CVSS 8.3 (CVE-2026-42941 and CVE-2026-42929), alongside CVE-2026-40425 (5.7), CVE-2026-42951 and CVE-2026-44611 (both 5.4). CISA states that successful exploitation "could result in an attacker gaining administrator access to the device"; the remediation is to update to firmware version V5.250.

What this means: A CISA advisory naming a specific shipboard navigation/data-recording system by model is rare and worth attention — VDRs sit on the bridge network, are frequently poorly segmented from other shipboard systems, and hold the authoritative evidentiary record after any collision, grounding or attack. Administrator-level

compromise of a VDR could allow tampering with or erasure of that record and potential pivoting across the bridge LAN. Fleet operators and DPAs should ask their VDR vendor or integrator three questions now: is installed firmware below V5.250, is the VDR's management interface reachable from any networked or remote-support path, and what is the upgrade timeline. The fix is firmware V5.250 — confirm affected units are scheduled for that build.

Test your response: Drill a bridge-OT failure where navigation and data-recording systems can no longer be trusted →

Source: CISA Advisory ICSA-26-148-01 | Date: 28.05.2026 | Credibility: High Additional sources: JVN / JPCERT VU#92172885, CISA ICSA-26-148-01, OpenText Vulnerability Vault — CISA advisories 28.05.2026

[VULNERABILITY] 6. CISA releases seven ICS advisories (19.05) hitting port and terminal OT — ScadaBR root RCE (CVSS 9.8), ZKTeco CCTV auth-bypass (CVSS 9.1), Siemens RUGGEDCOM, ABB, Kieback & Peter — CISA bulletin

[Regulatory: USCG MTS Rule | n/a] [Asset: Port OT | Corporate IT | Supply Chain]

[HIGH] On 19.05.2026 CISA released seven ICS advisories (five new plus two updates) under the bulletin "CISA Releases Seven Industrial Control Systems Advisories": ICSA-26-139-01 (ABB CoreSense HM and CoreSense M10 sensors), ICSA-26-139-02 (Siemens RUGGEDCOM APE1808 — a hardened application/network appliance widely used in substation and industrial networks), ICSA-26-139-03 (ScadaBR — a web-based SCADA platform; CVE-2026-8603, an OS command-injection flaw rated CVSS 9.8 that allows an unauthenticated remote attacker to execute commands as root on the SCADA host, alongside a companion hard-coded-credentials issue), ICSA-26-139-04 (ZKTeco CCTV cameras — CVE-2026-8598, a CVSS 9.1 authentication-bypass via an undocumented configuration-export port that requires no authentication and exposes camera credentials and service details), and ICSA-26-139-05 (Kieback & Peter DDC building controllers), plus updates to ICSA-24-177-01 (ABB 800xA Base) and ICSA-25-196-02 (ABB RMC-100).

What this means: These are general ICS/OT products rather than maritime-specific systems, but three of them sit squarely on the port-CISO patch path — ScadaBR (process-control automation found in tank farms, utilities and terminal support systems), ZKTeco CCTV (perimeter and terminal surveillance, often tied into access control), and Siemens RUGGEDCOM (the network backbone of many substation and terminal OT environments). The ScadaBR 9.8 unauthenticated-root flaw and the ZKTeco 9.1 auth-bypass are exactly the kind of internet-exposable defects that turn a convenience remote-access path into an open door. Port and terminal operators should inventory affected devices, pull management interfaces off the public internet and behind VPN/jump hosts, run SCADA under non-root accounts, and prioritise these in the next change window. The recurring governance lesson: you cannot triage a multi-vendor advisory batch inside 48 hours without an authoritative OT asset inventory.

Test your response: Test your team's ability to detect and isolate a compromised SCADA or access-control system at a port terminal →

Source: CISA (USDHSCISA bulletin) | Date: 19.05.2026 | Credibility: High Additional sources: NVD CVE-2026-8603 (ScadaBR), NVD CVE-2026-8598 (ZKTeco), JVNDB mirror 2026-05-19, Viakoo Daily OT Security News

---

Section 4: Ports and Supply Chain

No discrete port or terminal cyber incident meeting the credibility and event-date criteria fell into this category during the 16–31.05.2026 reporting period. The window's port and supply-chain cyber developments were governance- and threat-driven rather than incident-driven: the intensifying Baltic GNSS interference now reaches Finnish port approaches and pilotage waters (see Item 2), the CISA 19.05 advisory batch sits squarely on terminal-OT patch paths (Item 6), and NIS2 enforcement increasingly treats large EU seaports as in-scope essential entities (Item 4). The standing Sjöfartsverket and USCG NAVCEN advisories for Baltic and Black Sea GNSS interference remained in force throughout the period.

Section 5: People, Training and Governance

[REPORT] 7. UNITAR convenes Maritime Cyber Lab 2026 in Brussels — UN and IAPH frame port and supply-chain cyber resilience as a governance problem — UNITAR

[Regulatory: NIS2 | n/a] [Asset: Port OT | Supply Chain | Corporate IT]

On 27–28.05.2026 the United Nations Institute for Training and Research (UNITAR), together with the International Association of Ports and Harbors (IAPH) and with support from the German Federal Foreign Office, ran "Maritime Cyber Lab 2026: From Risk to Resilience" at UN House Brussels (in-person and online). The Lab examined cyber incidents in the maritime sector and threats to ports, port facilities and vessels; operational disruption and cascading supply-chain effects; and governance and coordination gaps across public and private actors — explicitly aligned with IMO cyber-risk guidance and EU frameworks including NIS2 and the Critical Entities Resilience (CER) Directive. The target audience spanned policymakers, maritime authorities, industry leaders, CISOs, financial institutions, international organisations and universities, and participation was free.

What this means: A UN-convened, IAPH-backed maritime cyber forum signals that port and supply-chain cyber resilience is consolidating as a governance topic at the intergovernmental level, not merely a technical one. For port authorities and operators the framing matters: "active resilience" built from training, institutional coordination and rehearsed incident response, sitting on top of NIS2/CER obligations. The Lab's outputs are worth tracking as a reference point for how regulators and intergovernmental bodies expect ports to demonstrate cyber maturity.

Source: UNITAR | Date: event 27–28.05.2026 (announced 17.03.2026) | Credibility: High

---

Section 6: Upcoming Maritime Cyber Events

Posidonia 2026 | 01–05.06.2026 | Athens (Metropolitan Expo), Greece World's largest shipping exhibition, with an expanded "Digital Shipping" hall and dedicated cyber, ROI, insurance-reduction and charter-party compliance tracks. Link

Port Performance Summit 2026 | 01–02.06.2026 | São Paulo, Brazil Leading Latin American event for port and terminal technology — automation, AI, IoT and cyber-resilience of port and PCS systems. Tentative date. Link

Digital Baltic 2026 | 02–04.06.2026 | Gdynia, Poland International conference on digital security in the Baltic Sea region — critical-infrastructure protection, dual-use technologies and NATO–EU cooperation against the backdrop of sustained Russian GNSS interference. Link

17th NMIOTC Annual Conference | 03–04.06.2026 | Souda Bay, Crete, Greece NATO high-security conference on hybrid threats — GPS spoofing, cyber attacks on ports as a prelude to kinetic action, and state-level adversaries. Link

MARSEC COE 6th International Maritime Security Conference | 09–10.06.2026 | Istanbul, Türkiye Annual NATO Maritime Security Centre of Excellence conference covering cyber threats to naval and commercial shipping, hybrid warfare at sea and critical maritime infrastructure protection. Link

Lloyd's Maritime Academy Certificate in Maritime Cyber Security | 09.06–31.08.2026 | Online Multi-week structured certificate programme for managers and officers covering regulatory context, technical and organisational controls and incident-response governance. Link

Maritime Cyber Guild Meetup Q2 | 15.06.2026 | Prague (Vienna House by Wyndham Diplomat), Czechia Grassroots practitioner meetup on the theme "What happens when cybersecurity fails?" — business continuity, disaster recovery, war-gaming and scenario planning. Link

CO2 Shipping & Terminals | 16.06.2026 | London, United Kingdom Conference on the security of OT systems for carbon-capture storage and transport — emerging cyber challenges in green shipping. Link

Autonomous Ship Expo 2026 | 16–18.06.2026 | Amsterdam (RAI), Netherlands Dedicated to unmanned vessels: control-link integrity, anti-jamming navigation, ethical AI decision-making and cyber as safety-critical engineering — directly relevant to the MASS Code adopted at MSC 111. Link

Monaco Energy Boat Challenge — Advanced Yachting Technology Conference | 08–11.07.2026 | Monaco (Yacht Club de Monaco) 13th edition; the Advanced Yachting Technology Conference (09.07) features panels on cyberattacks in yachting and GNSS "dark zones," AI weather routing and generative AI in yacht design. Invitation only. Link

Recent Events — late May 2026

International Tug & Salvage Convention | 19.05.2026 | Europe (TBD)
Conference focusing on tug telemetry security and operational-technology protection in specialised maritime operations. Tentative date. Link

Cyber Onboard 2026 | 26–27.05.2026 | Presqu'île de Giens, Hyères, France
Two-day specialist event on maritime OT cybersecurity covering shipboard systems, offshore platforms and port infrastructure, with emphasis on zero-trust access control for legacy navigation and control systems and compliance with class cyber rules. Link

---

Report compiled: 02.06.2026 | Coverage period: 16.05–31.05.2026 | 7 verified developments; multi-source verified across Tier 1–5. Lighter incident volume reflects a genuine post-Hormuz lull; items dated outside the window (Jan/March 2026, 2024) were excluded on event-date grounds.