Maritime Cybersecurity News Digest

Period: 01.05–15.05.2026

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 01–15.05.2026 fortnight was dominated by the second phase of the Iran war. On 04.05.2026 the United States launched Project Freedom to escort commercial vessels through the Strait of Hormuz; within 48 hours Iran fired cruise missiles, drones and small boats at commercial shipping nine times, the Panama-flagged HMM Namu sustained a fire after an "external strike by an unidentified flying object," and Iranian drones and missiles struck the VTTI oil terminal at Fujairah — a "direct hit between the GPS terminal and berths" per MEES — closing the UAE's principal Hormuz bypass route. By 06.05.2026 maritime intelligence firm Windward described Fujairah as the target of "a series of coordinated cyber and military strikes," with UAE crude exports plunging 58% to 1.35 million barrels per day and 100+ vessels stranded at anchorage. The operation was paused 05–06.05.2026 by mutual agreement, the Marshall Islands Maritime Administrator raised Ship Security Level to SSL 3 across the Middle East Gulf on 14.05.2026, and the Joint Maritime Information Center retained a CRITICAL regional threat assessment on 12.05.2026. In parallel, LockBit 5.0 listed Yang Ming Marine Transport's German arm on its leak portal on 07.05.2026, CISA released five new ICS advisories on 05.05.2026 (Hitachi Energy PCM600, ABB B&R PVI/Runtime/Studio, Johnson Controls CEM AC2000) and launched its CI Fortify initiative the same day, urging critical-infrastructure operators — including port and terminal operators — to assume threat actors will have access to their OT networks and to plan for sustained isolated operation. Iranian state media (Press TV) explicitly claimed responsibility for the HMM Namu strike on 06.05.2026 even as Iran's embassy in Seoul denied it.

[INCIDENT] 1. HMM Namu hit by external strike in Strait of Hormuz — Iran's embassy denies, Press TV claims attack — Reuters via Al-Monitor

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

[CRITICAL] On 04.05.2026 the Panama-flagged container ship MV HMM Namu, operated by South Korean line HMM, was struck while transiting the Strait of Hormuz. The vessel was carrying 24 crew, who were unharmed; the strike caused a fire and "damage to the lower stern hull" after two unidentified objects impacted the ship at one-minute intervals — a pattern consistent with a targeted strike. The vessel was brought to Dubai for forensic investigation. On 06.05.2026 Iran's state-run Press TV stated "We targeted a South Korean vessel that violated maritime regulations… a clear signal that Iran will exercise its sovereign rights through kinetic action"; the same day, Iran's Embassy in Seoul "firmly rejected and categorically denied" any Iranian military involvement. US President Donald Trump publicly attributed the strike to Iran and urged Seoul to join Operation Project Freedom. On 12.05.2026 the South Korean government formally announced the cause as "an external strike by an unidentified flying object" without naming an attacker. By 13–14.05.2026 a senior official at South Korea's Ministry of Foreign Affairs told Yonhap that any actor other than Iran was "unlikely" responsible and confirmed Seoul was analysing US-shared intelligence on the strike. As of mid-May, +26 South Korean vessels and +160 South Korean crew members remain stranded inside the Arabian Gulf.

What this means: The HMM Namu is the first publicly attributed kinetic strike on a third-country container vessel in the post-Epic Fury phase of the Iran war and is the operational reason large numbers of mariners remain trapped inside the Gulf. The diverging signals from Tehran (formal denial + state-media claim of responsibility) are themselves an information-warfare control surface — they raise insurance costs while preserving ambiguity

for cargo-owner and charter-party disputes. Where attribution is contested (mine vs missile vs USV), forensic chain-of-custody — onboard CCTV, AIS event logs, ECDIS playback, satcom and VHF DSC records — becomes the decisive evidence.

Source: Reuters / Yonhap (via Al-Monitor) | Date: 13.05.2026 | Credibility: High Additional sources: Al Jazeera / Anadolu Agency, Chosun Biz, Dawn, Chosun Editorial 12.05.2026

Test your response: Run a tabletop on ambiguous-attribution incident response when bridge systems and onboard OT are damaged in a contested-waters transit →

[INCIDENT] 2. Iranian strikes on Fujairah VTTI oil terminal — direct hit between GPS terminal and berths, +100 vessels stranded, exports collapse 58% — MEES

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

[CRITICAL] On 04.05.2026, hours after the United States launched Project Freedom to reopen the Strait of Hormuz, Iran launched a coordinated aerial barrage at the United Arab Emirates that included 12 ballistic missiles, three cruise missiles and four drones, according to UAE air-defence assessments. The Fujairah Petroleum Industries Zone was hit, with a drone striking the VTTI oil terminal — a facility jointly owned by IFM Global Infrastructure Fund, Vitol Group and Abu Dhabi National Energy Company (TAQA). Per MEES sources on 08.05.2026, the main strike was "a direct hit — rather than falling debris — between the GPS terminal and berths, causing significant damage to the pipeline near the manifold." Three Indian nationals were hospitalised. ADNOC suspended its 922 000 bpd Fujairah processing operation; a second strike hit the ADNOC-affiliated tanker M.V. Barakah by two drones in the Strait of Hormuz. On 06.05.2026 Windward described the Fujairah disruption as "a series of coordinated cyber and military strikes," recording 470 vessels affected by GPS jamming off Fujairah in 24 hours (three new jamming clusters), 167 vessels near Hormuz with 146 operating dark and stationary, +100 commercial vessels stranded at anchorage, and a drop in UAE crude exports to 1.35 million barrels per day — a 58% decline against the ten-year seasonal average. Storage operators at Fujairah (Vopak, VTTI, MENA and GPS) had already suspended operations and restricted staff access prior to the strike. The Habshan–Fujairah pipeline, the principal UAE Hormuz-bypass route, was indirectly impaired.

What this means: Fujairah's strategic value was that it allowed UAE crude to be loaded east of the Strait of Hormuz, eliminating chokepoint risk. The 04–05.05.2026 strikes destroyed that escape valve: a kinetic strike on the VTTI terminal, GPS infrastructure damaged on land, and 470 vessels electronically blinded offshore in 24 hours. For energy-shipping CISOs, the case study is the convergence of physical and cyber attacks on a single asset — the pipeline manifold, the GPS terminal, and the surrounding waterspace all degraded simultaneously. Resilience planning for Hormuz-bypass infrastructure should now assume coordinated multi-vector attacks rather than discrete kinetic or cyber events.

Source: MEES | Date: 08.05.2026 | Credibility: High Additional sources: WANA (Windward summary), Reuters via The Star, WorldOil / Bloomberg, Offshore Technology, Argus Media

Test your response: Practice your incident response when a port terminal sustains a combined cyber-physical attack on storage, pipelines, and onboard navigation systems →

[INCIDENT] 3. Project Freedom launches in Hormuz, pauses in 48 hours — Iran fires at commercial shipping nine times, seizes two container ships — Breaking Defense

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

[HIGH] On 03.05.2026, US President Donald Trump announced Project Freedom, a US-led operation — distinct from Operation Epic Fury — to guide commercial vessels safely through the Strait of Hormuz. CENTCOM commenced the mission on 04.05.2026 with guided-missile destroyers, +100 land- and sea-based aircraft, multi-domain unmanned platforms and 15 000 service members. Two US-flagged merchant vessels and a Maersk-affiliated vessel (Alliance Fairfax) transited under US military overwatch. CENTCOM commander Admiral Brad Cooper described the operation as "inherently a defensive operation," confirming US forces destroyed six Iranian small boats

and intercepted Iranian cruise missiles and drones. Within 48 hours Iran fired at commercial vessels nine times and seized two container ships, with attacks on US forces +10 times. A French-company-operated vessel attempting an unauthorised transit was hit, with crew injuries reported. On 05–06.05.2026 Trump announced Project Freedom was paused "by mutual agreement" as ceasefire negotiations continued; per the NNPC Marine circular of 11.05.2026, active US escorting of commercial ships was suspended while the US blockade of Iranian ports remained in force. On 05.05.2026 CENTCOM reported 22 500 mariners on +1550 commercial vessels trapped in the Arabian Gulf. Per Lloyd's List, shipowners and insurers found the US package failed to provide "sufficient clarity or credible protection" to justify resuming transits.

What this means: Project Freedom is, in effect, a stress test of whether US-government convoy intelligence, war-risk underwriting and naval overwatch are sufficient to overcome commercial-shipping risk aversion. Two days of operation showed they are not. For maritime CISOs and DPAs whose vessels are still inside the Arabian Gulf, the practical guidance is to treat any Hormuz transit decision as multi-stakeholder (master, DPA, charterer, P&I, war-risk underwriter, flag state) and to refresh standing voyage-plan triggers — including GNSS denial procedures, AIS-off contingencies, and crew-protection measures — before the next transit window.

Source: Breaking Defense | Date: 04.05.2026 | Credibility: High Additional sources: Operation Project Freedom (Wikipedia), CENTCOM Press Release, Fortune, Times of Israel, Insurance Journal 08.05.2026, NNPC Marine circular 11.05.2026

Test your response: Walk your fleet through a major-chokepoint contested-transit scenario with mixed kinetic and electronic warfare threats →

[GNSS] 4. Windward "Maritime Visibility Collapses" — 470 ships GPS-jammed off Fujairah, 146 dark vessels near Hormuz, MSC Francesca still detained — Windward

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

[**HIGH**] On 06.05.2026 maritime intelligence firm Windward published a special brief documenting a sharp deterioration in maritime visibility around the Strait of Hormuz in the 48 hours after Project Freedom launched. Specific findings include: +470 vessels affected by GPS jamming off Fujairah in 24 hours and three new jamming clusters identified; 167 vessels detected near Hormuz on 05.05.2026 by satellite imagery, of which 146 were operating dark and stationary; four dark vessels detected loading at Iran's Kharg Island primary crude export terminal despite enforcement pressure; the MSC Francesca containership (Aponte-family-owned MSC, seized by IRGC on 22.04.2026 along with the Technomar-owned Epaminondas) intercepted after suppressing its AIS transponder, illustrating "the dilemma operators face between targeting exposure and detention risk." Windward also confirmed the HMM Namu strike likely deliberate after IRGC issued direct warnings to the vessel's anchorage zone, and tracked the Fujairah infrastructure damage that caused crude exports to collapse from 3.5–4 million barrels daily to approximately 500 000 barrels.

What this means: Windward's 06.05 telemetry is the clearest single snapshot of why the Hormuz–Fujairah corridor has become operationally unviable for most commercial traffic: navigation data cannot be trusted, AIS-off creates new compliance and seizure risk, and the boundary between offshore vessel disruption and onshore terminal disruption has effectively dissolved. Fleet operators should treat the 470 / 146 / 4 figures as the new baseline for the next transit window and assume that any AIS suppression — even when locally rational for crew safety — will be read by Iranian forces as cause for boarding under the new IRGC "maritime regulations" framework.

Source: Windward | Date: 06.05.2026 | Credibility: High Additional sources: ZeroHedge / Bloomberg 05.05.2026, Insurance Journal 08.05.2026

Test your response: Simulate a contested-transit incident where ECDIS, AIS and ship's position cannot be independently verified →

[INCIDENT] 5. LockBit 5.0 lists Yang Ming Marine Transport's German arm on leak portal — HookPhish (ransomware.live mirror)

[Regulatory: NIS2] [Asset: Corporate IT]

[HIGH] On 07.05.2026 at 15:26 UTC, the LockBit 5.0 ransomware operation added de.yangming.com — the German division of Yang Ming Marine Transport Corporation, the Taiwanese container line ranked among the top ten globally by capacity — to its data-leak portal, threatening to publish exfiltrated data unless the company opened negotiations. The listing was discovered and indexed by ransomware-tracking infrastructure at 16:13 UTC the same day. LockBit 5.0 — the claimed successor to LockBit 3.0 after Operation Cronos dismantled the original infrastructure in February 2024 — has emerged as one of the most active ransomware-as-a-service operations of 2026, with 262 victims documented at the time of the Yang Ming listing. The group's tradecraft includes double-extortion, multi-platform encryptors (Windows, Linux and VMware ESXi) and a 30-day countdown before public data release. Yang Ming has not publicly confirmed operational impact on its German freight operations. The listing came in the same week the German Federal Ministry of the Interior announced (13.05.2026) plans for "active cyberdefence" legislation in response to a 10% year-on-year increase in ransomware against German organisations.

What this means: Container-line subsidiaries operating in EU Member States sit squarely inside NIS2 scope for water-transport entities and supply-chain risk. A leak-portal listing — even before encryption — triggers the 24-hour early-warning obligation under NIS2 Article 23, the 72-hour full-notification window, and the 30-day final-report requirement. CISOs at multinational shipping lines should expect each national-subsidiary listing now generates a parallel NIS2 reporting workstream in every EU jurisdiction with an in-scope entity. Pre-built playbooks per Member State (CSIRT contacts, language requirements, escalation channels) materially reduce response time.

Source: HookPhish / ransomware.live | Date: 07.05.2026 | Credibility: Medium Additional sources: DeXpose, cybercrime.works LockBit 5.0 tracker, Ransomware.live Germany map, Germany active cyberdefence (The Star)

Test your response: Walk through a NIS2-clock incident response when a national subsidiary is named on a leak portal but operational impact is unclear →

Section 2: Regulations & Standards

[REGULATION] 6. Marshall Islands raises required Ship Security Level to SSL 3 for Hormuz / Gulf of Oman / Northern Arabian Sea — Republic of the Marshall Islands SSA-2026-03

[Regulatory: IMO MSC.428] [Asset: Shipboard OT | Corporate IT]

[HIGH] On 14.05.2026 the Republic of the Marshall Islands Maritime Administrator issued revised Ship Security Advisory SSA-2026-03, applicable to all RMI-flagged vessels transiting or intending to transit the Middle East Gulf (MEG), Strait of Hormuz, Gulf of Oman, Northern Arabian Sea, Red Sea, Bab el-Mandeb and Gulf of Aden. The advisory raised the required Ship Security Level to SSL 3 (severe/critical) for the MEG, Gulf of Oman, Strait of Hormuz and Northern Arabian Sea, and SSL 2 (moderate/substantial) for the Red Sea, Bab el-Mandeb and Gulf of Aden. The framework operationalises Project Freedom (announced 03.05.2026, commenced 04.05.2026, paused 05–06.05.2026) and JMIC Advisory Note 004-26 (issued 04.05.2026). RMI noted NAVCENT's establishment of a Maritime Warning Zone covering the MEG, Gulf of Oman, Northern Arabian Sea and Strait of Hormuz, and stated explicitly that NAVCENT cannot guarantee the safety of merchant vessels within the designated area. The advisory revised threat levels for the Northern Red Sea from CRITICAL to MODERATE and the Southern Red Sea from CRITICAL to SUBSTANTIAL.

What this means: RMI is the world's third-largest open registry and SSL 3 is a binding operational instruction — not advisory guidance — to RMI-flagged masters. Cargo owners, charterers, P&I clubs and reinsurers should expect (a) higher manning, watchkeeping and hardening costs per transit, (b) more frequent VHF queries from coalition forces and (c) potential refusal-to-transit decisions backed by flag-state authority. Other major registries (Liberia, Panama, Singapore, Hong Kong) are likely to mirror RMI's SSL escalation in the next 7–14 days; voyage planners should pre-position cyber-resilient navigation procedures (paper charts, secondary GNSS receivers, celestial backup) regardless of flag.

Source: Republic of the Marshall Islands | Date: 14.05.2026 | Credibility: High Additional sources: JMIC Advisory Update 041 12.05.2026 (Albawheels Up)

[REGULATION] 7. Joint Maritime Information Center retains CRITICAL threat level for Strait of Hormuz, sustains MARAD 2026-004 guidance — Albawheels Up / JMIC Advisory Update 041

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

On 12.05.2026 the Joint Maritime Information Center — operated by NAVCENT and partner navies — published Advisory Update 041 retaining the CRITICAL regional threat level for the Strait of Hormuz, citing the 03.05.2026 attack on a commercial vessel near Iranian waters. JMIC kept the Somali Basin at SEVERE (three merchant vessels currently held by pirates), the Southern Red Sea / Bab el-Mandeb at SUBSTANTIAL and the Northern Red Sea / Suez Canal at MODERATE. The advisory reiterated MARAD Advisory 2026-004 (Hormuz, in force through 09.09.2026): vessel operators must (a) avoid responding to diversion instructions from unverified sources, (b) maintain a minimum 30 nautical-mile standoff from US naval vessels, (c) continuously monitor VHF Channel 16, and (d) immediately report suspicious activity to UKMTO. JMIC noted that, while GNSS/AIS interference levels are below the March 2026 peaks, sporadic electromagnetic interference persists near Cyprus and parts of the Levant.

What this means: US- and partner-flagged vessels should treat JMIC 041 + MARAD 2026-004 + RMI SSA-2026-03 + the JMIC Advisory Note 004-26 procedural framework as a coherent risk envelope for the next transit window. Where flag-state SSLs and MARAD guidance overlap, default to the more restrictive instrument.

Source: Albawheels Up / JMIC | Date: 12.05.2026 | Credibility: Medium

---

[REGULATION] 8. CISA Cyber Incident Reporting (CIRCIA) final rule targeted for May 2026 — 72-hour incident reporting and 24-hour ransomware payment reporting on the horizon — Nelson Mullins Cyber Brief

[Regulatory: USCG MTS Rule | NIS2] [Asset: Corporate IT | Port OT | Shipboard OT]

Legal commentary published 03.05.2026 confirms that CISA's final rule implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is targeted for adoption in May 2026, introducing two new mandatory obligations for covered critical-infrastructure entities (including Marine Transportation System entities under MTSA): a 72-hour timeline for reporting covered cyber incidents and a 24-hour timeline for reporting ransom payments. The commentary was issued in the context of a 07.04.2026 joint advisory by CISA, FBI, NSA, DOE, EPA and US Cyber Command (AA26-097A) flagging an active Iranian-affiliated APT campaign against US critical infrastructure exploiting internet-exposed Rockwell/Allen-Bradley programmable logic controllers in the water, wastewater, energy and government-facilities sectors. CSIS analysis (12.05.2026) noted that the CISA campaign attribution maps to the "CyberAv3ngers" group affiliated with the IRGC Cyber-Electronic Command, which since 2023 has compromised at least 75 core automation devices in US critical infrastructure.

What this means: US-flagged vessel, OCS and MTSA-regulated facility operators should not wait for the final CIRCIA rule before refreshing incident-response plans. Three concrete steps before the rule lands: (1) confirm that monitoring and escalation processes generate alerts the right people actually see and respond to; (2) hold an incident-response refresher covering escalation paths, legal/insurance notification rules, and out-of-band communications (phone trees, alternative email, Signal) in case primary systems are down; (3) pre-identify outside counsel and confirm cyber-insurance policy notice requirements so there is no delay when the 24/72-hour clock starts.

Source: Nelson Mullins | Date: 03.05.2026 | Credibility: High Additional sources: CSIS 12.05.2026, SecurityWeek 07.04.2026 (Iranian PLC advisory)

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

[VULNERABILITY] 9. CISA publishes five new ICS advisories on 05.05.2026 — Hitachi Energy PCM600, ABB B&R PVI/Runtime/Studio, Johnson Controls CEM AC2000 — Cyber Centre Canada AV26-441

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

[HIGH] On 05.05.2026 CISA released five new ICS advisories: ICSA-26-125-01 (Hitachi Energy PCM600 — control and protection system used in substation automation, common in port-side energy management), ICSA-26-125-02 (ABB B&R PVI — visualization runtime, versions prior to 6.5.0), ICSA-26-125-03 (ABB B&R Automation Runtime — versions prior to 6.5 and prior to R4.93), ICSA-26-125-04 (ABB B&R Automation Studio — versions prior to 6.5), and ICSA-26-125-05 (Johnson Controls CEM AC2000 — physical access control system widely deployed at port and terminal entry points, including ship-to-shore crane control rooms; affected versions 12.0, 11.0 and 10.6). CISA also issued updates for ICSA-23-227-01 (Schneider Electric EcoStruxure Control Expert and Modicon M340/Momentum/MC80/M580 family — Update A) and ICSA-24-319-16 (Hitachi Energy MSM — Update A). The new advisories were independently catalogued by Canada's Cyber Centre under serial AV26-441 (11.05.2026) and re-broadcast through JVN/JPCERT on 07–08.05.2026.

What this means: Three of the five new advisories — Hitachi Energy PCM600 (substation feeds), ABB B&R Automation Runtime (PLC/automation stacks) and Johnson Controls CEM AC2000 (physical-access gateways) — sit directly on the port-CISO patch path. Port operators should treat these advisories as immediate scope for their next change window, with priority given to (a) network segmentation between business networks and crane-control / access-control networks, (b) multifactor authentication on all remote access into PLC and access-control environments, and (c) physical asset-inventory reconciliation against installed firmware versions. The Schneider Modicon M580 update is particularly relevant given that variant of the M580 family is referenced in MARAD 2026-007 port-crane guidance.

Source: Cyber Centre Canada | Date: 11.05.2026 | Credibility: High Additional sources: JVN/JPCERT 07.05.2026, SecuaLive (English JVN mirror), Scannetsecurity 11.05.2026

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

[OT] 10. CISA launches CI Fortify — operators must assume threat actors have OT-network access and plan for "weeks to months" of isolated operation — Industrial Cyber

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

On 05.05.2026, CISA — under acting director Nick Andersen — launched CI Fortify, an "allied initiative" directing critical-infrastructure operators (water utilities, electricity providers, transportation operators including ports, healthcare) to prepare for cyber-degraded operations during geopolitical conflict. The guidance is built on two emergency planning objectives: **isolation** (proactively disconnecting OT from third-party dependencies and operating without reliable telecommunications, internet, vendors and upstream services) and **recovery** (documenting system operation, backing up critical files, practising replacement and manual-mode transitions). CISA's baseline planning assumption is explicit: "Operators should assume that in a conflict scenario third-party connections… will be unreliable and that threat actors will have some access to the OT network." Isolation guidance specifies that operators should identify "critical customers" (e.g. nearby military bases), set service-delivery targets, and maintain business-continuity plans "for weeks to months." CISA confirmed it has begun a pilot phase of "targeted assessments" of participating operators' resilience measures. The initiative is modelled on Australian government guidance from 2025.

What this means: For port and terminal operators, CI Fortify reframes the legacy IT-OT segmentation discussion as a "manual-mode readiness" question: can your gate, your crane fleet, your TOS, your bunkering schedule, your VTS feed all run without WAN connectivity for a defined number of hours, days or weeks — and have you actually rehearsed it end-to-end? Boards and audit committees should ask for a documented isolation-and-recovery rehearsal

in 2026 — not a tabletop, an end-to-end simulation with the network physically pulled. The "service delivery target for critical customers" framing is particularly relevant for ports serving naval bases, oil-and-gas export terminals and pharmaceutical supply chains.

Source: Industrial Cyber | Date: 06.05.2026 | Credibility: High Additional sources: Nextgov, CybersecurityDive, Inside Cybersecurity 05.05.2026, AHA 06.05.2026, TechTarget 07.05.2026, Crowell client alert 14.05.2026

Test your response: Practice operating your port or fleet for hours without internet, IT systems or remote support →

[REPORT] 11. CSIS — Iranian cyber threat to US critical infrastructure is now "weaponising existing access," operates in water and energy "comfort zone" — CSIS Analysis

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

On 12.05.2026, the Center for Strategic and International Studies (CSIS) published an analysis of recent CISA, FBI, NSA, DOE, EPA and US Cyber Command joint advisory AA26-097A (07.04.2026) on Iranian-affiliated cyber activity against US critical infrastructure. CSIS makes five operational observations: (1) the activity represents Iran "weaponising existing access" to US networks established as far back as January 2025; (2) the actors operate in Iran's "comfort zone" — water, wastewater and energy facilities — using low-sophistication methods exploiting basic vulnerabilities (default passwords, internet-exposed PLCs); (3) the campaign extends beyond pure disruption into espionage, access maintenance and information operations; (4) historical patterns suggest "noise-level" attacks (causing localised damage to victims) will continue throughout the conflict; (5) the CyberAv3ngers group affiliated with the IRGC Cyber-Electronic Command has compromised at least 75 core automation devices in US critical infrastructure since 2023. CSIS notes that CISA is operating at approximately 38% staffing during this period — complicating the agency's coordination capacity at exactly the moment Iranian operations are escalating.

What this means: For maritime CISOs in the United States, the immediate implication is that exposure of port-side OT (cranes, gates, bunkering, water/power supply to terminals) to the public internet via "convenience" remote-access pathways is no longer a defensible architectural choice. The Iranian PLC campaign exploits Rockwell/Allen-Bradley devices through ports 44818, 2222, 102, 22 and 502; port-side OT teams should grep their network maps for any such device with inbound exposure and remediate before the next incident-report deadline. The thinly-staffed CISA also means MTS operators should expect slower federal response and should pre-establish private-sector incident-response retainers.

Source: CSIS | Date: 12.05.2026 | Credibility: High Additional sources: Nelson Mullins Cyber Brief 03.05.2026, SecurityWeek 07.04.2026

Section 4: Ports and Supply Chain

[REPORT] 12. NAVCEN GUIDE logs only one marine GPS-interference incident in the 01–15.05 period — vessel transiting Japan to Vancouver lost GPS 70 NM south of Japan — USCG NAVCEN GUIDE

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

Between 01.05.2026 and 15.05.2026, the USCG NAVCEN GPS User Issue Detection & Evaluation (GUIDE) tool recorded a single marine GPS interference incident: report #971, dated 06.05.2026, from a commercial sailing vessel transiting Japan to Vancouver that experienced "loss of GPS signal 70 NM south of the coast of Japan." NAVCEN closed the case as "Unknown Interference" on 11.05.2026, finding no GPS constellation anomalies, no space-weather correlation, no authorised GPS testing in the area and no corroborating inter-agency reports. This absence of new Baltic and Black Sea NAVCEN entries during the period contrasts sharply with the dense April 2026 logging (entries #960 Black Sea / Midia Romania, #963–964 MV MAJ RICHARD WINTERS IMO 9210309 Baltic Sea / Gulf of Gdansk near Kaliningrad). The standing Sjöfartsverket NAVTEX warnings 026/25 (Baltic GNSS, AIS, radar,

DGPS interference) and 016/26 (The Sound — GPS interference) remained in force throughout the period, as did the FlySafe Baltic GPS Jamming Live Tracker assessment that interference is persistent across Finland, Estonia, Latvia, Lithuania, Northern Poland, Slovakia and Sweden.

What this means: The drop-off in formal NAVCEN reports for the Baltic and Black Sea in early May likely reflects under-reporting fatigue rather than diminished interference — coastal-state NAVTEX warnings remain active and the underlying Russian electronic-warfare network described in the December 2025 Gdańsk Maritime University / GPSPATRON study is structurally unchanged. Fleet operators should maintain Baltic GNSS-loss procedures, log every event to NAVCEN (https://www.navcen.uscg.gov/report-a-problem), and treat the absence of fresh entries as a reporting gap rather than an operational improvement.

Source: USCG NAVCEN | Date: 11.05.2026 (case closure date) | Credibility: High Additional sources: Sjöfartsverket Navigational Warnings, FlySafe Baltic GPS Jamming Tracker

---

Section 5: People, Training and Governance

No incident or report meeting the credibility and date-window criteria fell into this category during the 01–15.05.2026 reporting period. Standing references — Marlink Cyber Intelligence Report 2026 (14.04.2026), Cydome Maritime Trends Report 2026 (03.2026), CYTUR sector playbooks (23.03.2026) and BIMCO Guidelines on Cyber Security Onboard Ships — remain authoritative governance frameworks for the period but are not new events.

Section 6: Upcoming Maritime Cyber Events

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

Port Performance Summit 2026 | 01–02.06.2026 | São Paulo, Brazil Leading Latin American event for port and terminal technology, focusing on automation, AI, IoT and cyber-resilience of port and PCS systems across Brazilian and regional ports. Link

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

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. Link

Recent Events — May 2026

EM-ISAC Annual Meeting | 01.05.2026 | Rotterdam, Netherlands
Annual European Maritime ISAC meeting — cyber threat information sharing for EU ports and maritime operators. Link

Offshore Technology Conference (OTC) 2026 | 04–07.05.2026 | Houston, USA
World's premier offshore technology conference — critical-infrastructure cybersecurity, digital solutions and marine energy. Link

People Tech Maritime — Hamburg (Hamburg Maritime Forum) | 05–06.05.2026 | Hamburg, Germany
Focus on scaling cybersecurity across large managed fleets — endpoint protection deployment challenges. Link

GISEC Global 2026 | 05–07.05.2026 | Dubai, UAE
Middle East's largest cybersecurity expo. Critical Infrastructure track covered SCADA security for oil terminals and OT assets in extreme environments. Link

Digital@Sea North America | 06–07.05.2026 | Florida, USA
Focus on the security of digital navigation data and communications, e-navigation standards and implementation. Link

BIMCO Cyber Online | 11.05.2026 | Online
Legal- and risk-oriented online seminar covering shipping digitalisation, OT and navigation cyber threats, the BIMCO Cyber Security Clause 2019, liability allocation and cyber insurance. Link

CMI Rio 2026 — Maritime Law Conference | 12–15.05.2026 | Rio de Janeiro, Brazil
International Maritime Committee colloquium covering maritime violence and fraudulent activity, including cyber-enabled fraud, MASS legal framework and maritime governance. Link

RiskTech Marine 2026 | 13.05.2026 | London (Lloyd's Building), United Kingdom
One-day conference at Lloyd's focused on how cyber, climate, operational and regulatory pressures are reshaping marine risk, with panels on OT/IT cyber safety, vessel-port integration resilience and AIS/GPS manipulation. Link

Maritime IT Networking Summit 2026 | 13–14.05.2026 | Grecotel La Riviera, Peloponnese, Greece
Two-day curated B2B summit bringing together shipping company IT/digital leaders and solution providers for one-to-one meetings, keynotes and roundtables on maritime IT, digitalisation and cybersecurity strategy. Link

- **Premium:** Intelligence Brief (this report) — semi-monthly deep-dive, multi-source verified. See plans →

Questions or feedback? contact@ogmios.pl

Report compiled: 17.05.2026 | Coverage period: 01.05–15.05.2026 | Sources: 64 unique sources across Tier 1–5