# Maritime Cybersecurity News Digest

**Period: 16.04–30.04.2026**

---

**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 16–30 April 2026 window saw the Strait of Hormuz crisis escalate from a single US naval blockade into a dual blockade after Iran re-closed the strait on 18 April, stranding +2000 vessels and reducing traffic to roughly 5% of the pre-war baseline. ShinyHunters claimed a major data breach against Carnival Corporation / Holland America Line (8.7 million records, 7.5 million unique emails leaked after ransom deadline passed). On the OT side, the Copy Fail Linux kernel vulnerability (CVE-2026-31431) emerged as the most impactful single-CVE event for maritime OT in 2026 — a deterministic root exploit affecting +22 confirmed maritime systems from VSAT terminals to port cranes, with a type-approval patch gap measured in months. Forescout's BRIDGE:BREAK research disclosed 22 vulnerabilities in serial-to-IP converters used in port crane controls and RTUs, while CISA released +38 ICS advisories across the fortnight. On the regulatory front, IMO FAL 50 advanced mandatory cybersecurity for Maritime Single Windows and Singapore Maritime Week delivered the OCEANS-X platform and a dedicated Maritime OT Cybersecurity Programme.*

---

### [GNSS] 1. Strait of Hormuz dual blockade — Iran re-closes strait as GNSS/AIS interference persists, +2000 ships stranded — Al Jazeera

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

**[CRITICAL]** On 18.04.2026, Iran re-closed the Strait of Hormuz to all foreign-flagged vessels in response to the United States refusing to lift its naval blockade. The result is a dual blockade with no modern precedent. +2000 ships remain stranded in the Gulf. Between 17 and 26 April, roughly 66 commercial vessels transited the strait — mostly from states Iran deems "friendly" (China, India, Thailand, Malaysia) — against a pre-war baseline of +138 per day. Iran has been charging a reported $2 million toll per transit, payable in Chinese Yuan or cryptocurrency. A DeepDraft special brief from 16 April describes Hormuz entering a "forensic enforcement" phase, with GNSS interference extending into timing desynchronisation across bridge systems, AIS ghosting and false vessel signatures in the Kish–Abu Musa sector, and degraded digital navigation on key approaches requiring manual navigation, inertial systems and radar correlation. Windward analysis identifies at least 30 jamming clusters across Saudi Arabia, Kuwait, UAE, Qatar, Oman and Iran. US MARAD advisory 2026-004 (Hormuz theatre) warns US-flagged vessels to prepare for active GNSS interference and ignore diversion orders, while MARAD advisory 2026-006 (Red Sea theatre) urges caution and AIS measures. Iran's shadow fleet continues using fake flags, shell companies and disabled tracking signals to evade the US blockade.

**What this means:** The dual blockade transforms the Hormuz crisis from a military standoff into a protracted maritime data integrity problem: vessel operators cannot rely on AIS position reports, insurance underwriters face unprecedented claims complexity, and the shift to permission-based transit regimes creates a two-tier navigation environment where commercial intelligence about which vessels are actually moving — and where — is itself degraded. MARAD 2026-004 and 2026-006 should be treated as standing guidance for all Gulf and Red Sea transits.

Source: Al Jazeera | Date: 18.04.2026 | Credibility: High Additional sources: CNN, Bloomberg, The National, Fortune, DeepDraft, RadarCell

**Test your response:** Practice navigating a dual-blockade GNSS spoofing scenario where vessel positions and AIS data cannot be trusted →

---

**[INCIDENT] 2. ShinyHunters claims Carnival Corporation / Holland America Line breach — 8.7 million records, 7.5 million unique emails leaked — The Register**

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

**[HIGH]** On 18.04.2026, the extortion group ShinyHunters listed Carnival Corporation on its pay-or-leak portal, claiming the theft of 8.7 million records from Holland America Line's Mariner Society loyalty programme — a Carnival subsidiary. The exposed data includes names, dates of birth, genders, membership status and at least 7.5 million unique email addresses. ShinyHunters set an April 21 deadline for ransom negotiations; when Holland America did not engage, the group published the data, stating "The company failed to reach an agreement with us despite our incredible patience." Carnival confirmed it detected suspicious activity tied to a phishing incident involving a single user account and engaged external cybersecurity experts. ShinyHunters — previously responsible for high-profile breaches of AT&T, Ticketmaster and +40 other companies — has a documented track record of following through on leak threats.

**What this means:** Cruise operators holding passenger PII at scale remain high-value targets for extortion groups. The entry vector here — a single phished account — shows that MFA and privileged access controls on loyalty platform backends are not optional hardening; they are the baseline.

Source: The Register | Date: 24.04.2026 (claim listed 18.04.2026) | Credibility: High Additional sources: Security Boulevard, Seatrade Cruise, TechRadar

**Test your response:** Simulate your shipping company's response to a ransomware attack targeting corporate systems and vessel operations →

---

**[REPORT] 3. RIN Maritime GNSS Interference Working Group survey: 75% report no improvement, 85% experience receiver failures — Shipping Telegraph**

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

**[HIGH]** On 17.04.2026, the Royal Institute of Navigation (RIN) Maritime GNSS Interference Working Group published a survey confirming that GNSS disruption across major shipping corridors — the Baltic Sea, Strait of Hormuz, Red Sea, Black Sea and Eastern Mediterranean — remains a critical operational challenge with no meaningful improvement. 75% of survey respondents reported that interference conditions have not improved, and 85% of affected vessels experienced GNSS receiver failures, with 20% requiring manual power cycling to restore functionality. The survey additionally documents that GNSS interference is increasingly compromising secondary systems including ECDIS and AIS, which depend on GPS-derived timing and positioning data, elevating collision risk in contested and congested waters. Concrete April cases confirm the RIN findings: USCG NAVCEN logged the US merchant vessel MV MAJ RICHARD WINTERS (IMO 9210309) experiencing GPS jamming and spoofing in the Baltic Sea at 0220 on 18.04.2026, 10 NM ENE of the Baltica offshore wind farms — positions were spoofed eastward onto Russian territory near Kaliningrad, affecting all onboard GPS-dependent systems including two JRC GP-170 receivers, the GNSS compass, both Inmarsat-C terminals, AIS and VHF DSC (NAVCEN ID 964). A separate NAVCEN entry (ID 962) from the same date logs unexplained GPS loss from a vessel in the Red Sea, classified as "Unknown Interference" with no constellation anomalies or space weather factors.

**What this means:** The combination of RIN survey data and real-time NAVCEN incident logs confirms that GNSS interference is a structural condition across major trade routes, not a temporary disruption — fleet operators should treat receiver resilience testing, backup PNT procedures, and ECDIS/AIS independence from sole GPS input as standing requirements for all vessels transiting affected corridors. The Baltic incident — with spoofed positions pointing toward Russian territory — is consistent with the January 2026 joint warning from 14 Baltic and North Sea coastal states attributing growing GNSS interference to Russia.

Source: Shipping Telegraph | Date: 17.04.2026 | Credibility: High Additional sources: USCG NAVCEN GUIDE, Neptune P2P OSINT

---

**[INCIDENT] 4. MTS-ISAC warns of credential-harvesting phishing operations targeting maritime organisations — Cydome Maritime Cybersecurity Bulletin**

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

On 17.04.2026, Cydome's Maritime Cybersecurity Bulletin reported that MTS-ISAC issued a warning about active credential-harvesting phishing operations targeting maritime personnel and organisations. The campaigns use lures specifically designed to steal identities and gain access to fleet management, port operations and logistics systems. The warning aligns with Marlink's April Cyber Intelligence Report data showing that 82% of maritime cyber incidents in 2025 originated in crew network zones, with phishing and credential theft as dominant entry vectors — and with less than 11% of users reporting suspicious activity.

**What this means:** Maritime organisations should treat the MTS-ISAC phishing warning as a direct indicator to refresh phishing simulation programmes, enforce multi-factor authentication across all fleet and port management platforms, and review whether crew and shore-staff reporting channels are functioning and incentivised.

Source: Cydome / MTS-ISAC | Date: 17.04.2026 | Credibility: High

**Test your response:** Explore how compromised credentials and insider behaviour enable network-wide compromise in our stowaway tabletop →

---

## Section 2: Regulations & Standards

---

**[REGULATION] 5. IMO FAL 50 outcomes: mandatory cybersecurity for Maritime Single Windows — amendments for FAL 51 adoption — DNV**

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

The 50th session of the IMO Facilitation Committee (FAL 50), held in late March 2026, approved amendments to the FAL Convention requiring contracting governments to implement mandatory cybersecurity measures to protect Maritime Single Windows (MSWs) — the electronic port clearance platforms that facilitate vessel arrival, departure and cargo documentation. The amendments, reported by DNV and IAPH in early April, will be submitted for formal adoption at FAL 51 in 2027, with entry into force expected 01.01.2029. The session also initiated work on a non-mandatory, goal-based Maritime Cyber Code with a target completion date of 2028 — complementing the +40 state proposal for a binding code submitted at MSC in early April. IAPH confirmed that its proposal on mandatory cybersecurity was adopted by the Committee.

**What this means:** FAL 50 moves maritime cybersecurity from voluntary guidelines to binding requirements for a specific system category. Port authorities and MSW operators should start mapping their current architecture against the incoming requirements, with authentication, data integrity and incident response for clearance workflows as the obvious first targets.

Source: DNV | Date: FAL 50 session March 2026; outcomes reported April 2026 | Credibility: High Additional sources: IAPH, Smart Maritime Network, Bureau Veritas

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

---

**[REGULATION] 6. Singapore launches Maritime OT Cybersecurity Programme and OCEANS-X platform at SMW 2026 — MPA Singapore**

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

During Singapore Maritime Week (20–24.04.2026), the Maritime and Port Authority of Singapore (MPA), together with the Singapore Shipping Association (SSA), Singapore Institute of Technology (SIT) and Singapore University of Technology and Design (SUTD), announced the Cybersecurity for Maritime Operational Technology programme — a dedicated two-month course for corporate IT professionals in shipping companies, covering key shipboard


OT systems and their interface with shore-based operations. Participants will receive hands-on training using the MariOT simulator at SUTD's iTrust Centre to manage cyber incidents in simulated maritime environments, with the first cohort starting August 2026. Separately, MPA launched OCEANS-X, a new data and API exchange platform establishing secure system-to-system connectivity across the maritime ecosystem to support port services resilience.

**What this means:** Singapore is now building maritime cyber capability, not just publishing policy. The OT training programme and OCEANS-X platform together create a template that other major port states should look at as they work through NIS2 and USCG compliance.

Source: MPA Singapore | Date: 21.04.2026 | Credibility: High Additional sources: Safety4Sea, Smart Maritime Network

---

**[REGULATION] 7. USCG Maritime Cyber Rule — operational lessons and CySO readiness guidance published — Vogel IT-Law Blog**

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

On 17.04.2026, legal and practitioner analysis published in response to the USCG Cybersecurity in the Marine Transportation System rule distilled operational lessons for maritime CISOs and facility operators. The analysis emphasises three key milestones: mandatory cyber-incident reporting to the National Response Center (effective 16.07.2025), completion of workforce cybersecurity training for all personnel with IT/OT access (deadline passed 12.01.2026), and designation of a Cybersecurity Officer (CySO) plus full cyber risk assessment and plan submission (due 16.07.2027). For foreign-flag ships, the guidance underscores that poor cyber hygiene affecting ISM Code compliance may trigger Port State Control actions including deficiencies, detention or denial of entry — extending the rule's practical reach beyond US-flagged vessels.

**What this means:** With the training deadline already passed and the CySO/plan deadline 14 months away, the April guidance serves as a mid-cycle reality check: operators who have not yet begun designating CySOs and structuring their assessment programmes are now running against an increasingly compressed timeline, with PSC enforcement risk rising for non-compliant vessels calling at US ports.

Source: Vogel IT-Law Blog | Date: 17.04.2026 | Credibility: High Additional sources: The Maritime Executive

**Test your response:** Practice responding to a USCG cyber inspection with failing OT systems and regulatory gaps →

---

**[REGULATION] 8. NIS2/IEC 62443 alignment emerging as OT compliance benchmark for ports and maritime terminals — Secra**

[Regulatory: NIS2] [Asset: Port OT | Shipboard OT]

On 29.04.2026, an analysis by Secra tied the April 2026 wave of CISA ICS advisories to the broader NIS2 compliance landscape, arguing that IoT/OT security has become a mainstream enterprise and regulatory risk rather than a niche control engineering concern. The analysis positions IEC 62443 as the emerging de facto standard for demonstrating NIS2 compliance across OT-heavy essential sectors — including ports and maritime terminals — and argues that April's advisory volume (+38 ICS advisories across the fortnight) constitutes evidence that regulators expect OT-level controls, not just IT-centric measures, for NIS2 compliance. The piece specifically frames the convergence of USCG MTS Rule requirements, IMO MSC.428, IACS UR E26/E27 and IEC 62443 as creating a "multi-standard compliance surface" that port and vessel operators must manage simultaneously.

**What this means:** Port and terminal operators under NIS2 should look at IEC 62443 as their OT compliance framework rather than trying to stretch IT-centric controls across industrial environments. The overlap between USCG, IMO, IACS and NIS2 requirements is large enough that a single compliance architecture can serve multiple frameworks if planned from the OT layer up.

Source: Secra | Date: 29.04.2026 | Credibility: Medium


**Test your response:** Navigate a NIS2 compliance crisis triggered by ransomware in our regulatory tabletop exercise →

---

## Section 3: OT/ICS Threats & GNSS/PNT

---

**[VULNERABILITY] 9. Copy Fail (CVE-2026-31431) — deterministic Linux kernel root exploit affects +22 confirmed maritime systems from bridge to crane — copy.fail**

[Regulatory: IACS E26/E27] [Asset: Shipboard OT | Port OT | Satcom/VSAT | Corporate IT]

[**CRITICAL**] On 28.04.2026, a security researcher published a 732-byte Python proof-of-concept script exploiting CVE-2026-31431 ("Copy Fail") — a vulnerability in the Linux kernel's algif_aead cryptographic module, shipped enabled by default since 2017, that grants any unprivileged local user deterministic root access. The exploit is not probabilistic: the same script works across Ubuntu, RHEL, SUSE, Amazon Linux and Debian with no per-system tuning. It bypasses read-only filesystems, secure boot and container isolation by corrupting the in-memory page cache rather than on-disk files. An Ogmios Maritime analysis identified 22 confirmed Linux-based maritime systems across 9 categories exposed to Copy Fail, from vendors including Cobham (SAILOR 900 VSAT), Moxa (industrial networking), Danelec (VDRs), Honeywell (Enraf CIU 888 tank gauging), ZPMC (port cranes), Navis (N4 terminal operating system at +250 ports), KVH, Intellian, MAN Energy Solutions and Westermo. Eight of these 22 systems have documented SSH or shell access with known default credentials. For Navis N4, Copy Fail chains with a separately disclosed CISA vulnerability (CVE-2025-2566, CVSS 9.8 — unauthenticated Java deserialization RCE) to provide zero-credential-to-root on the dominant container terminal operating system. A C port of the exploit removing the Python 3.10 requirement already exists on GitHub, making embedded systems directly exploitable.

**What this means:** Copy Fail is the most significant single-CVE exposure event for maritime OT in 2026. The patch gap between IT-managed servers (days) and OEM-locked, type-approved systems like VDRs, VSAT terminals and engine controls (6–12 months) means the fleet and port attack surface will remain open for an extended period. Immediate compensating controls — disabling algif_aead where possible, changing default credentials on VSAT terminals, segmenting OT networks from crew Wi-Fi and vendor VPNs — are available and effective.

Source: copy.fail / CERT-EU Advisory 2026-005 | Date: 28.04.2026 | Credibility: High Additional sources: CERT-EU, CISA Navis N4 advisory

**Test your response:** Simulate a destructive attack leveraging root access on vessel Linux systems in our wiper tabletop exercise →

---

**[OT] 10. BRIDGE:BREAK — Forescout discloses 22 vulnerabilities in serial-to-IP converters enabling OT disruption and lateral movement — Industrial Cyber**

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

[**HIGH**] On 22.04.2026, Forescout published the BRIDGE:BREAK research disclosing 22 vulnerabilities in widely deployed serial-to-IP converters manufactured by Lantronix and Silex Technology — the "glue" devices that bridge legacy serial-based PLCs and RTUs to IP networks in industrial environments. The vulnerability cluster includes unauthenticated access, buffer overflows and hard-coded credentials, enabling attackers to tamper with data passing between serial OT devices and IP networks, take over converter devices, and create lateral movement pathways deeper into OT networks. CISA issued advisory ICSA-26-111-10 for affected Silex devices in its 21–23 April advisory batch. For maritime and port operators, these converter classes are commonly embedded in crane controls, RTUs, tank gauging systems, yard management systems and rail interfaces — which puts BRIDGE:BREAK squarely on port OT teams' patch lists.

**What this means:** Port OT teams should inventory all serial-to-IP converters in their environments, cross-reference against the BRIDGE:BREAK CVE list, and implement compensating controls (network segmentation, access

restrictions) where patching is not immediately possible; the research demonstrates that these “invisible” bridging devices represent a systemic weak point in IT/OT segmentation architectures.

Source: Industrial Cyber / Forescout | Date: 22.04.2026 | Credibility: High Additional sources: CISA ICS Advisory ICSA-26-111-10

**Test your response:** Simulate a cyber-physical attack exploiting OT network weaknesses in safety-critical port systems →

---

**[VULNERABILITY] 11. Fortinet patches critical FortiSandbox vulnerabilities — CVE-2026-39813 and CVE-2026-39808, both CVSS 9.1, PoC public — Help Net Security**

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

**[CRITICAL]** On 16.04.2026, Fortinet disclosed 27 new vulnerabilities across its product portfolio, including two critical flaws in FortiSandbox: CVE-2026-39813 (path traversal in the JRPC API allowing authentication bypass) and CVE-2026-39808 (OS command injection allowing unauthenticated remote code execution), both scoring CVSS 9.1. A public proof-of-concept exploit for CVE-2026-39808 is available, significantly increasing the risk of opportunistic exploitation. Multiple national CERTs issued advisories, including Singapore’s Cyber Security Agency (CSA). FortiSandbox is deployed by maritime Security Operations Centres and managed security providers — including Marlink Cyber’s SOC network — for malware analysis and threat detection across fleet and port environments, which means a FortiSandbox compromise can blind the very SOC watching the fleet.

**What this means:** Maritime SOCs and managed security providers running FortiSandbox should treat this as an emergency patching priority; until upgraded to FortiSandbox 4.4.9+ or 5.0.6+, organisations should restrict JRPC API exposure, monitor for exploitation indicators, and assess whether sandbox analysis workflows may have been compromised during the exposure window.

Source: Help Net Security | Date: 16.04.2026 | Credibility: High Additional sources: SecurityWeek, Singapore CSA

---

**[OT] 12. CISA ICS advisory surge — +38 advisories in April 16–30 covering ABB, Siemens, Cisco, Mitsubishi and transport systems — CISA / WaterISAC**

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

**[HIGH]** CISA pushed an unusual volume of ICS advisories in the 16–30 April window: 18 advisories on 21–23 April spanning 11 vendors (including Siemens, Silex Technology, Milesight and others), 12 advisories on 28 April, and 8 more on 30 April covering ABB Ability Symphony Plus, Mitsubishi Electric products and additional vendors. Notable for maritime operators: the 23 April batch includes an update for **Schneider Electric Modicon M340/M580/Quantum/MC80 controllers** — widely deployed in port cranes, pumping stations and cargo-handling systems — with vulnerabilities allowing remote code execution, denial of service or loss of control logic integrity. Advisory ICSA-26-120-01 (30 April) addresses critical Denial-of-Service vulnerabilities in the **ABB IEC 61850 MMS communication stack** used in System 800xA and Symphony Plus — frequently deployed in port-side power management, shore power systems and terminal substation automation. The 30 April batch also covers **Mitsubishi Electric MELSEC EtherNet/IP modules** and FA products used in conveyor systems, gates and packaging equipment at ports. Separately, on 20.04.2026, CISA added eight vulnerabilities to its KEV catalog including Cisco Catalyst SD-WAN Manager flaws (CVE-2026-20122, CVE-2026-20128) under active exploitation — relevant to ship-to-shore and corporate maritime routing infrastructure. On the perimeter side, SonicWall issued advisory SNWLID-2026-0004 on 29 April for three SonicOS vulnerabilities (CVE-2026-0204/0205/0206) affecting Gen6/7/8 firewall lines — including access control bypass, path traversal and buffer overflow — a problem for any maritime network relying on SonicWall at the perimeter.

**What this means:** The April advisory volume, combined with active Cisco SD-WAN exploitation and fresh SonicWall flaws, creates a concentrated patching burden. Priority order for port OT teams: Schneider Modicon and ABB IEC 61850 for automation, Cisco SD-WAN KEVs for ship-to-shore routing, SonicWall for Gen6-8 perimeter

firewalls. If your organisation still lacks a structured OT vulnerability management programme, this month's advisory count is reason enough to build one.

Source: CISA / WaterISAC | Date: 21–30.04.2026 | Credibility: High Additional sources: Canadian Centre for Cyber Security, CyberPress

---

**[GNSS] 13. Orca AI analysis: managing navigation risk under persistent Hormuz GNSS degradation — +1650 vessels affected — Orca AI**

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

On 28.04.2026, Orca AI published an analysis of navigation risk under the persistent GNSS degradation in the Strait of Hormuz and Persian Gulf. It describes widespread GPS spoofing conditions where vessels appear miles inland on ECDIS displays, jump erratically on tracking systems and report impossible positions in AIS feeds — conditions affecting +1650 vessels in the region since the February 2026 escalation. The piece reinforces that GNSS disruption has driven crews to treat satellite positioning as just one input among several, relying more heavily on radar, AIS correlation, visual navigation and manual cross-checks. It references MARAD MSCI 2026-004 and JMIC updates characterising the interference as persistent and deliberate, with direct implications for collision risk and incentives for vessels to operate AIS-dark to avoid targeting.

**What this means:** The Hormuz GNSS problem has moved from acute crisis to chronic condition. Fleet safety managers should use this analysis as a reference for updating bridge standing orders and PNT backup procedures. Crews also need to understand that other vessels going AIS-dark to avoid targeting increases collision risk on top of the GNSS degradation itself.

Source: Orca AI | Date: 28.04.2026 | Credibility: High

**Test your response:** Practice bridge team decision-making under GPS spoofing where AIS data cannot be trusted →

---

**[THREAT] 14. Joint US advisory AA26-097A: Iranian APT actors actively exploiting Rockwell/Allen-Bradley PLCs in critical infrastructure — CISA**

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

**[HIGH]** Joint US advisory AA26-097A, published 07.04.2026 by FBI, CISA, NSA, EPA, DOE and US Cyber Command, warns that Iranian-affiliated APT actors (CyberAv3ngers / IRGC Cyber Electronic Command, also tracked as Storm-0784 and Bauxite) are actively exploiting internet-facing Rockwell Automation / Allen-Bradley programmable logic controllers — specifically CompactLogix and Micro850 families — in US critical infrastructure since at least March 2026. The actors use legitimate Rockwell Studio 5000 Logix Designer software to interact with project files and manipulate HMI/SCADA displays, causing operational outages without requiring zero-day exploitation. Censys telemetry identifies 5219 internet-exposed hosts on EtherNet/IP (port 44818) self-identifying as Rockwell/Allen-Bradley devices. While the advisory is sector-agnostic, the same PLC families and HMI/SCADA architectures are deployed in port power distribution, pumping systems, cargo handling equipment and terminal automation. The advisory's timing — amid the broader Iran-US Hormuz confrontation — means maritime critical infrastructure operators should treat Iranian APT targeting of industrial control systems as an elevated and concurrent threat.

**What this means:** Port operators using Rockwell/Allen-Bradley PLCs should immediately audit internet-facing exposure of their PLC and HMI infrastructure, verify that default credentials have been changed, and implement network segmentation between PLC networks and corporate IT; the convergence of kinetic conflict (Hormuz blockade) and targeted ICS exploitation (AA26-097A) creates a compound threat environment for Gulf-adjacent and US port infrastructure.

Source: CISA AA26-097A | Date: 07.04.2026 (exploitation ongoing through April) | Credibility: High Additional sources: Censys, Picus Security


## Section 4: Ports & Supply Chain

**[REPORT] 15. WEF and Port of Rotterdam: port cyber risk is now ecosystem-wide — collective defence model needed — Industrial Cyber**

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

On 20.04.2026, the World Economic Forum, in collaboration with the Port of Rotterdam, published an analysis warning that rapid digitalisation has transformed port cyber risks from isolated operational issues into systemic, ecosystem-wide vulnerabilities. The analysis notes that attacks increasingly move laterally across shipping lines, terminals and logistics providers, rendering traditional siloed security models ineffective. It advocates replacing individual-entity security postures with a "collective cyber defence" model where port authorities, terminal operators, carriers and government agencies share threat intelligence and coordinate incident response. The Dutch Ferm Seaports initiative — a public-private intelligence-sharing platform operational since 2025 across Rotterdam, Amsterdam and Antwerp — is highlighted as a blueprint for executing shared defence across competing commercial entities.

**What this means:** The WEF analysis gives port authorities and NIS2-regulated entities a framework for justifying investment in shared threat intelligence and coordinated response. The Ferm Seaports model is the closest working example of what this looks like in practice; European port clusters and US MTS-ISAC members should study it.

Source: Industrial Cyber / WEF | Date: 20.04.2026 | Credibility: High Additional sources: SC World

**[REPORT] 16. Kpler analysis: AIS spoofing vs GNSS interference — why the distinction decides the insurance claim — Kpler**

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

On 27.04.2026, Kpler published an analysis of why the distinction between AIS spoofing and GNSS interference is critical for maritime insurance claims — and why conflating the two leads to incorrect coverage frameworks, wrong evidentiary standards and misallocated liability. For passive GNSS interference, the operative framework is the Institute War & Strikes Clauses, JWC Listed Area provisions and the Additional War Risk Premium (AWRP) mechanism, with IWSC Clause 5 seven-day cancellation rights. When electronic interference is classified as a cyber peril rather than a war risk, an entirely different clause set applies. The analysis emphasises that the AIS record from an interference period is unreliable by definition, and that claims reconstruction must rely on VDR records, non-GPS positioning streams and independent surveillance data. With +1650 disruption events recorded in the Gulf region since February 2026, the financial stakes of correct classification are significant.

**What this means:** Marine insurers, P&I clubs and claims handlers should use the Kpler framework to audit their current classification practices for Hormuz-related claims; vessel operators should ensure their VDR data retention and non-GPS positioning logs are complete and accessible, as these will carry the evidentiary weight in disputed claims where AIS records are degraded.

Source: Kpler | Date: 27.04.2026 | Credibility: High

## Section 5: People, Training & Governance

**[GOVERNANCE] 17. DNV and Equinor launch CLUE incident learning taxonomy — eliminating hindsight bias in maritime cyber incident analysis — DNV**

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

On 17.04.2026, DNV and Equinor launched the Contextual Learning & Understanding of Events (CLUE) taxonomy — a structured framework for improving how the maritime and energy sectors analyse and communicate safety and cybersecurity incidents. CLUE focuses on system conditions that shaped outcomes rather than assigning blame to individual decisions. It records insights from failures and successes alike, and standardises how incident context is shared between organisations. The timing matters: maritime cyber incidents doubled year-on-year, and the same patterns (crew phishing, OT lateral movement, GNSS manipulation) keep showing up at different operators. A common language for incident learning is overdue.

**What this means:** Fleet operators and port authorities running post-incident reviews should look at CLUE as a complement to existing root cause analysis. The system-conditions focus is a better fit for maritime environments, where crew actions during cyber incidents are typically shaped by bad procedures, poor network visibility or conflicting system outputs rather than personal error.

Source: DNV | Date: 17.04.2026 | Credibility: High

---

## Section 6: Upcoming Maritime Cyber Events

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

**People Tech Maritime — Hamburg** | 05–06.05.2026 | Hamburg, Germany 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 covers SCADA security for oil terminals and OT assets in extreme environments. Link

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

**BIMCO Digitalisation & Cyber Risks in Shipping Seminar** | 11.05.2026 | Online Legal- and risk-oriented online seminar covering OT and navigation systems, 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 addressing maritime violence, cyber-enabled fraud, MASS legal framework, and maritime governance. Link

**RiskTech Marine 2026** | 13.05.2026 | London, United Kingdom One-day conference at Lloyd's on cyber, climate, operational and regulatory pressures reshaping marine risk. Panels on OT/IT cyber safety and AIS/GPS manipulation. Link

**Maritime IT Networking Summit 2026** | 13–14.05.2026 | Peloponnese, Greece Curated B2B summit for shipping IT/digital leaders. One-to-one meetings, keynotes and roundtables on maritime IT, digitalisation and cybersecurity strategy. Link

**International Tug & Salvage Convention** | 19.05.2026 | Europe (TBD) Focus on tug telemetry security and operational technology protection in specialized maritime operations. Link

**Cyber Onboard 2026** | 26–27.05.2026 | Hyères, France Specialist event on maritime OT cybersecurity, covering shipboard systems, offshore platforms and port infrastructure. Emphasis on zero-trust access control for legacy navigation and control systems. Link

**Posidonia 2026** | 01–05.06.2026 | Athens, Greece The "Olympics of Shipping" — world's largest shipping exhibition. Expanded "Digital Shipping" hall with cybersecurity showcase. 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, NATO-EU cooperation. 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 prelude to kinetic action, state-level adversaries. Link

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

**Maritime Cyber Guild Meetup Q2** | 15.06.2026 | Prague, Czech Republic Grassroots practitioner meetup. Theme: "What happens when cybersecurity fails?" — business continuity, disaster recovery, war-gaming, scenario planning. Link

### Recent Events — April 2026

**DSA & NATSEC Asia 2026** (20–23.04.2026, Kuala Lumpur, Malaysia)
Asia's flagship defence and national-security exhibition with sea-based platform and offshore systems exhibits. C4ISR and cyber-related technologies for naval and maritime critical infrastructure. Link

**Singapore Maritime Week 2026** (20–24.04.2026, Singapore)
20th edition of Asia's largest maritime event. Hosted "Marine CyberSafe" forum, launched OCEANS-X platform and Maritime OT Cybersecurity Programme. Drew +20000 participants from 80 countries. Link

**People Tech Maritime — Athens** (21–22.04.2026, Athens, Greece)
Digitalization journey focus for Greek shipowners. Cyber security as enabler — cloud migration security, satellite network protection. Link

**Black Hat Asia 2026** (21–24.04.2026, Singapore)
Premier technical infosec event in Asia. Briefings segment featured new research on cyber-physical systems and maritime embedded systems. Link

**Sea Japan 2026** (22–24.04.2026, Tokyo, Japan)
Japan shipbuilding expo with "Digital Solution Square." Safety certification of AI-driven autonomous ships where cybersecurity is prerequisite for class approval. Link

**SMRC × MTEC/ICMASS Conference 2026** (22–23.04.2026, Singapore)
Research conference: "Smart Ships. Secure Seas. Sustainable Futures." MASS cyber-attack simulations and LEO satellite vulnerabilities in port and ship operations. Link

**Marine Insurance Asia** (23.04.2026, Singapore)
Cyber insurance policies for the maritime sector, risk assessment, and underwriting practices. CyberCube agentic AI findings discussed. Link

**Maritim Cyber Security 2026 — Ålesund** (30.04.2026, Ålesund, Norway)
GCE Blue Maritime Cluster forum on how NIS2 and IACS UR E26 drive concrete cybersecurity requirements for shipowners, operators, and suppliers. Link

### Stay ahead of maritime cyber threats

**Enjoyed this Intelligence Brief?** Get every issue delivered to your inbox.

- **Free:** Maritime Cyber Weekly — headline summaries, weekly. Subscribe →
- **Premium:** Intelligence Brief (this report) — semi-monthly deep-dive, multi-source verified. See plans →

Questions or feedback? contact@ogmios.pl


*Report compiled: 30.04.2026 | Coverage period: 16.04–30.04.2026 | Sources: 38 unique sources across Tier 1–5*