Maritime Cybersecurity News Digest

Period: 01.03–13.03.2026

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

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

Section 1: Incidents & Attacks

[INCIDENT] 1. Hacktivist group cuts 116 tankers off the internet via VSAT wipe — Hellenic Shipping News

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

[**HIGH**] The hacktivist group Lab Dookhtegan executed a high-impact operation on 02.03.2026, compromising a maritime connectivity provider and wiping VSAT partitions on hard drives aboard 116 tankers, severing all external communications. The attack represents a significant escalation in hacktivist capability — moving beyond defacement and data leaks to direct sabotage of shipboard communications infrastructure. All affected vessels lost access to remote fleet management, GMDSS-linked satellite services, and over-the-air software update channels simultaneously. The scale and method suggest advance reconnaissance of the provider's management plane rather than opportunistic exploitation.

What this means: Fleet operators sharing a single connectivity provider now face single-point-of-failure risk at the provider level; independent redundant satellite paths (e.g., LEO + GEO) and out-of-band emergency communication plans should be treated as non-optional.

Source: Hellenic Shipping News | Date: 02.03.2026 | Credibility: Medium Additional sources: Smart Maritime Network

Test your response: Practice a maritime ransomware crisis in our free tabletop exercise →

[INCIDENT] 2. AI-powered vishing surge — 1600% increase targeting shipping executives — Smart Maritime Network

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

[**HIGH**] A report published on 02.03.2026 documented a 1600% surge in AI-driven voice phishing (vishing) campaigns directed at shipping executives and shore-based crew management personnel. In one confirmed incident, a threat actor used AI-generated imagery and a stolen identity to pass video-based hiring verification, gain employment, and attempt server infiltration from inside the organisation via a "laptop farm." The attack methodology exploits the maritime sector's reliance on remote interviews for supernumerary and shore personnel, where physical identity verification is rarely performed. The barrier to entry for this class of attack has dropped sharply as synthetic voice and deepfake tooling becomes commodity-grade.

What this means: HR and identity verification processes for remote roles must now incorporate live liveness checks and document authentication; fleet managers should brief DPAs and crewing officers on AI-enabled social engineering as an active threat, not a theoretical risk.

Source: Smart Maritime Network | Date: 02.03.2026 | Credibility: Medium Additional sources: Hellenic Shipping News

---

[VULNERABILITY] 3. 60% of maritime software vulnerabilities weaponised within 48 hours via AI exploit generation — CIR Magazine

[Regulatory: IACS E26/E27] [Asset: Shipboard OT | Port OT | Supply Chain]

[CRITICAL] Research published on 03.03.2026 confirmed that 60% of newly disclosed software vulnerabilities affecting ship and port systems are now being weaponised within 48 hours of disclosure, driven by threat actors using AI to automate exploit generation at scale. The finding effectively collapses the traditional 30-day patching window that most fleet operators and port terminal operators have built into their change management processes. Systems with long patch cycles — including ECDIS chart management software, vessel management systems, and cargo handling applications — are disproportionately exposed. The research aligns with the broader trend of AI lowering both the cost and time-to-exploit across industrial control environments.

What this means: Patch management SLAs for internet-facing and OT-adjacent maritime systems must be revised from 30-day cycles to 48-hour emergency response for critical vulnerabilities; IACS E26/E27-compliant vessels should ensure their cyber risk management procedures reflect this accelerated threat tempo.

Source: CIR Magazine | Date: 03.03.2026 | Credibility: Medium

---

Section 2: Regulations & Standards

[REGULATION] 4. IMO MSC.428(98) enforcement: DOC withheld for companies without cyber risk management in SMS — Ship Universe

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

On 04.03.2026, the IMO reaffirmed the enforcement posture of Resolution MSC.428(98), clarifying that flag state administrations and recognised organisations are expected to withhold or suspend the Document of Compliance (DOC) for any company that cannot demonstrate cyber risk management integrated into its Safety Management System (SMS). Companies failing the annual DOC verification without evidence of a functioning cyber risk management programme now face immediate operational restrictions, including the potential withdrawal of certificates necessary to trade. The clarification follows a pattern of uneven implementation across flag states, with some accepting minimal paper-based cyber policies while others have begun conducting substantive audits. The resolution has been in force since 01.01.2021, meaning non-compliance is no longer attributable to transition-period uncertainty.

What this means: Shipowners and managers approaching DOC renewal audits in 2026 must ensure cyber risk management is documented, tested, and traceable within the SMS — generic cyber policy statements without operational evidence of implementation are increasingly being rejected by auditors.

Source: Ship Universe | Date: 04.03.2026 | Credibility: Medium

Test your response: Practice an IMO MSC.428 Port State Control cyber inspection →

[REGULATION] 5. EU Cybersecurity Act 2: ENISA to issue maritime ICT incident-response playbooks; satellite hardware flagged as "High-Risk Suppliers" — Global Policy Watch

[Regulatory: NIS2 | ENISA Port] [Asset: Satcom/VSAT | Corporate IT | Supply Chain]

Technical guidance released on 11.03.2026 on the Cybersecurity Act 2 proposal confirms that ENISA will be empowered to develop sector-specific incident-response playbooks for maritime ICT assets, covering vessel systems, port infrastructure, and satellite communications. The guidance also designates certain satellite communication hardware from specific vendors as "High-Risk Suppliers," triggering procurement restrictions analogous to the telecom sector's 5G supplier risk framework. EU member states operating major ports or registering significant

fleets under their flag will be required to align procurement and incident response with ENISA playbooks once the Act enters into force. The proposal extends supply-chain scrutiny to the maritime sector in a manner not previously formalised under existing EU cybersecurity legislation.

What this means: Port operators and shipowners procuring new VSAT or satellite navigation hardware in EU jurisdictions should begin supplier risk assessments now; the "High-Risk Supplier" designation, once finalised, may require costly equipment replacement or segregation measures on already-installed systems.

Source: Global Policy Watch | Date: 11.03.2026 | Credibility: Medium

Test your response: Practice handling a ransomware strike before a NIS2 compliance audit →

Section 3: OT/ICS Threats & GNSS/PNT

[GNSS] 6. Middle East Gulf: 672 daily GNSS interference events, +655 vessels affected by spoofing — Lloyd's List

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

[CRITICAL] Data published on 02.03.2026 shows daily GNSS interference events in the Middle East Gulf and Gulf of Oman have reached 672 incidents per day, with more than 655 vessels having experienced spoofing since the onset of regional hostilities. Primary hotspots are concentrated off the coasts of the UAE, Iran, and Oman, where spoofing signals are displacing vessel positions by distances sufficient to cause ECDIS-plotted tracks to show vessels inland or in waters inconsistent with their actual position. The affected region overlaps with some of the world's highest-density tanker traffic lanes, including the Strait of Hormuz approaches. Vessels relying solely on GNSS for position input to ECDIS without cross-referencing radar-derived positions or AIS correlation are at elevated grounding and collision risk.

What this means: Masters and officers transiting the Persian Gulf and Gulf of Oman should implement GNSS anomaly detection procedures — cross-checking GNSS position against independent sources (radar parallel indexing, celestial observations, LORAN-C where available) — and report position anomalies to maritime rescue coordination centres and flag state authorities.

Source: Lloyd's List | Date: 02.03.2026 | Credibility: High

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

[GNSS] 7. Baltic and Black Seas: Russian-origin GNSS interference "endemic" across 14 European states, disrupting GMDSS timing — CP24 / CNN

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

[HIGH] A joint warning issued on 06.03.2026 and covered by international media confirmed that GNSS interference in the Baltic Sea and Black Sea has reached endemic levels, with 14 European states formally warning their maritime communities of ongoing Russian-origin jamming and spoofing. Beyond navigational position errors, the interference is disrupting GMDSS timing systems, which depend on precise UTC time signals distributed via GPS; delays in GMDSS timing have in documented cases delayed rescue coordination by maritime rescue coordination centres. The geographic scope — spanning the Baltic approaches to the Danish Straits, the Gulf of Finland, and into the Black Sea — means that vessels transiting Northern European and Eastern European waters face near-continuous exposure. The interference pattern shows characteristics of both deliberate jamming (broadband suppression) and spoofing (false position injection).

What this means: Vessels transiting the Baltic and Black Sea should treat GNSS as degraded infrastructure and not as a sole means of position-fixing; DPAs and fleet managers should review whether vessels carry operational backup PNT equipment, and should flag GMDSS timing dependency on GPS as a residual risk in safety management system cyber risk assessments.

Source: CP24 / CNN | Date: 06.03.2026 | Credibility: Medium

Test your response: Practice navigating a Black Sea GPS spoofing incident →

[OT] 8. NORMA Cyber: 800% surge in attacks on edge devices bridging shipboard OT and IT networks — Smart Maritime Network

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

[HIGH] An advisory issued by NORMA Cyber on 02.03.2026 documented an 800% increase in cyberattacks targeting edge devices — routers, VPN concentrators, and firewalls — that form the boundary between shipboard OT networks and corporate IT or satellite communication links. The advisory states that "the most significant risk in 2026 comes from inside the perimeter," reflecting a shift in attacker focus from external breach attempts to exploitation of devices that, once compromised, provide persistent access to both sides of the IT/OT boundary simultaneously. Many shipboard edge devices run outdated firmware, lack centralised configuration management, and are not monitored by the same security tooling as corporate endpoints. The 800% figure represents a dramatic acceleration from the previous year's baseline and is consistent with broader ICS/OT threat intelligence trends reported by Dragos and CISA.

What this means: Fleet IT/OT managers must prioritise firmware inventory and vulnerability assessment for all shipboard edge devices as an immediate action; network segmentation that relies solely on a single firewall appliance at the IT/OT boundary is no longer adequate — additional monitoring, anomaly detection, and out-of-band management access should be implemented.

Source: Smart Maritime Network | Date: 02.03.2026 | Credibility: Medium

---

[VULNERABILITY] 9. ICRNSA advisory: automated steering systems vulnerable to spoofed NMEA data feeds — Conference Alerts

[Regulatory: IACS E26/E27] [Asset: Shipboard OT | PNT/GNSS]

A specialised advisory on Robotic Navigation Systems released on 10.03.2026 following the ICRNSA conference in Hamburg identified structural vulnerabilities in automated steering systems that consume NMEA 0183 and NMEA 2000 data bus feeds without integrity validation. Because the NMEA protocol does not include authentication or message integrity mechanisms, any attacker with access to the vessel's internal data network — or to the GNSS receiver's output — can inject falsified position, heading, or speed data into the autopilot or dynamic positioning system. The advisory noted that increasing deployment of autonomous and semi-autonomous vessels amplifies the attack surface, as these platforms depend more heavily on automated steering logic than conventionally crewed vessels. The vulnerability class is not new, but the ICRNSA findings update the threat model to include AI-assisted real-time spoofing that adapts injected data to vessel behaviour patterns.

What this means: Vessels with automated steering or dynamic positioning systems should audit NMEA data paths for unauthorised access points and consider implementing independent sensor cross-validation (e.g., comparing GNSS-derived heading with gyrocompass and radar-derived motion) as a compensating control.

Source: Conference Alerts / ICRNSA | Date: 10.03.2026 | Credibility: Medium

Test your response: Practice handling ECDIS and autopilot failures during a USCG inspection →

OGMIOS
Maritime Cybersecurity

Section 4: Upcoming Maritime Cyber Events

This section lists upcoming conferences/events in the next 6 weeks (until end of April 2026). Data from the Maritime Cybersecurity Conference Calendar.

MTS-ISAC Maritime Cyber Resilience Summit | 16–17.03.2026 | Athens, Greece Community-driven ISAC summit: real-time threat intelligence sharing, active defense, threat hunting on vessel networks. Link

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

Baltic Security Conference 2026 | 19.03.2026 | Riga, Latvia Largest Baltic security event — IT security, crisis management, physical security. Link

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

NORMA Cyber Conference 2026 | 24.03.2026 | Oslo, Norway Flagship Norwegian maritime cyber event. Launch of Annual Threat Assessment report; state-sponsored actors targeting Nordic maritime/energy. Link

Port of the Future Conference 2026 | 24–26.03.2026 | Houston, USA Future of ports — infrastructure, cybersecurity, automation across maritime, land, and cyber domains. Link

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

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

Smart Maritime Network Rotterdam | 15.04.2026 | Rotterdam, Netherlands Port Community Systems (PCS) security — attack on Rotterdam PCS could freeze European supply chains. Link

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

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

Black Hat Asia 2026 | 21–24.04.2026 | Singapore Technical infosec with research on Cyber-Physical Systems — hacks on ECDIS, AIS, maritime embedded systems. Link

Recent Events — March 2026

Cydome Maritime Cyber Trends Report 2026 | ~03.2026
Annual report: AI automating maritime sabotage at scale; business risk implications for C-suite.

MC3 Gdynia | 10–12.03.2026 | Gdynia, Poland
Polish Naval Academy: offshore platform protection, international cooperation on drone threats to maritime assets. Link

ICRNSA Hamburg | 02–03.03.2026 | Hamburg, Germany
Robotic Navigation Systems & Autonomous Security: satellite security convergence with maritime OT; NMEA vulnerability advisory.

Questions or feedback? contact@ogmios.pl

Report compiled: 13.03.2026 | Coverage period: 01.03–13.03.2026 | Sources: 8 unique sources across Tier 1–4