Maritime Cybersecurity News Digest

Period: 01.04–15.04.2026

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 01–15 April 2026 window was dominated by the Strait of Hormuz crisis and continued maritime electronic warfare across multiple theatres (Hormuz, Black Sea). Two confirmed kinetic strikes on Russian maritime assets (Syvash EW platform, Sheskharis oil terminal) and the Venice San Marco infrastructure breach round out the incident picture. Pure ransomware/extortion incidents against shipping lines or ports were notably absent from public reporting in this window — flagged transparently per editorial policy. Trend reports (Marlink, CYTUR) and regulatory milestones (IACS Rec 194, IMO Cyber Code proposal) defined the broader narrative.

[GNSS] 1. Strait of Hormuz ceasefire and US Navy blockade announcement — 4 transits/day as GNSS disruption continues — The Guardian / BBC

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

[CRITICAL] On 08.04.2026 the United States and Iran agreed to a two-week conditional ceasefire designed to reopen the Strait of Hormuz, followed on 13.04.2026 by a US Navy announcement of intent to blockade the Strait to clear mines and restore freedom of navigation. Despite the diplomatic development, GNSS and AIS interference — ongoing since late February 2026 and affecting +1100 vessels to date — remained active through the period: JMIC reporting for 11.04.2026 showed disruption moderating but still widespread, with merchant traffic constrained to approximately 4 transits per day against a historical average of ~138 per day. GPS signals affecting ship and VSAT positioning systems continued to be reported across UAE, Omani, and Iranian waters, with spoofed positions placing vessels at inland sites and airports.

What this means: The ceasefire and blockade announcement do not resolve the electronic warfare environment in the Strait; vessel operators must continue treating GNSS as an unreliable sole input, enforcing multi-source cross-checks (radar, gyrocompass, celestial) and briefing bridge teams that satcom outages in the region may reflect antenna GPS-dependency failures rather than hardware faults.

Source: The Guardian / BBC | Date: 08.04.2026 / 13.04.2026 | Credibility: High Additional sources: JMIC GNSS interference report 11.04.2026, Windward

Test your response: Practice navigating a multi-theatre GPS spoofing and satcom failure scenario in our free tabletop exercise →

[INCIDENT] 2. Ukrainian forces destroy Russian "Syvash" offshore platform used as GPS spoofing and surveillance relay hub — Ukraine RBC

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

[HIGH] On 06.04.2026, Ukrainian naval forces, the SBU, and unmanned systems destroyed the Syvash offshore gas platform in the Black Sea, which Russian forces had repurposed as an electronic warfare relay station. According to Ukrainian intelligence, the platform served as an active node for surveillance operations and GPS spoofing campaigns targeting Ukrainian vessel movements toward Crimea. Its destruction represents the first confirmed

kinetic elimination of a dedicated maritime GNSS disruption asset in the ongoing conflict and underscores that offshore and port-adjacent infrastructure can be militarised as electronic warfare nodes without physical modification to external appearance.

What this means: The Syvash strike highlights that GNSS disruption is not a passive side-effect of conflict — it is an active capability deliberately deployed from dedicated infrastructure; fleet security teams should treat persistent spoofing in contested theatres as evidence of intentional, resourced adversary operations rather than incidental interference.

Source: Ukraine RBC | Date: 06.04.2026 | Credibility: High

[INCIDENT] 3. Ukrainian long-range drones strike Sheskharis oil terminal at Port of Novorossiysk — Ukrainska Pravda

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

[HIGH] On 05–06.04.2026, Ukrainian long-range drone strikes targeted the Sheskharis oil loading terminal at the Port of Novorossiysk — Russia's largest Black Sea oil export hub — hitting energy infrastructure and terminal loading systems. While the attack was kinetic rather than cyber in execution, the strikes directly disrupted integrated digital systems for terminal management, loading automation, and cargo scheduling, forcing extended manual operations. The incident illustrates how physical attacks on maritime energy hubs achieve effects equivalent to a destructive cyberattack against OT systems, and reinforces the convergence of cyber-physical risk in contested port environments.

What this means: Port operators in geopolitically sensitive regions should review whether their OT resilience plans account for cyber-physical convergence scenarios where physical damage produces operational outcomes identical to a targeted cyberattack on terminal management or loading control systems.

Source: Ukrainska Pravda | Date: 06.04.2026 | Credibility: High

Test your response: Practice your port's operational continuity response when infrastructure fails suddenly →

[INCIDENT] 4. "Dark Engine" / "Infrastructure Destruction Squad" claims breach of Venice San Marco hydraulic flood control system — Security Magazine

[Regulatory: NIS2 (potential)] [Asset: Port OT | Corporate IT]

[HIGH] On 15.04.2026, a threat actor identifying as "Dark Engine" / "Infrastructure Destruction Squad" claimed administrative access to the hydraulic pump and flood control system protecting Venice's San Marco basin, publishing via Telegram channel system layout diagrams, control panel screenshots, and assertions that they held the capability to manipulate floodgates and valves to generate man-made floods. The group stated the breach began in late March 2026. Authorities had not confirmed the claim as of date of reporting. The target is a coastal critical infrastructure system with direct relevance to port operations: the same hydraulic management architecture controls waterway access for commercial vessels in the Venice lagoon port zone.

What this means: Coastal and port-adjacent hydraulic infrastructure — including tidal gates, lock controls, and basin water management systems — must be assessed as part of the maritime OT threat surface, not treated as separate civil engineering assets; this incident is a textbook case for the OT attack-on-safety-critical-systems tabletop scenario.

Source: Security Magazine | Date: 15.04.2026 | Credibility: High

Test your response: Simulate a cyber-physical attack on safety-critical port infrastructure in our OT tabletop exercise →

[REPORT] 5. Marlink Cyber Intelligence Report: 7793 incidents detected in 2025 — 82% in crew network zones — Marine Link

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

[HIGH] Published on 14.04.2026, the Marlink Cyber Intelligence Report documented 7793 detected cyber incidents across its monitored maritime fleet environments in 2025. A striking 82% of maritime security alerts originated in crew network zones rather than operational or bridge systems — with phishing and credential theft as the dominant entry points. Only 11% of users reporting suspicious activity indicates a severe gap in crew cyber awareness and reporting culture. The report further notes the persistent risk of lateral movement from crew networks into operational zones in vessels without robust IT/OT network segmentation.

What this means: The concentration of incidents in crew network zones combined with a less-than-11% reporting rate confirms that the human element remains the primary attack surface on connected vessels; fleet operators should prioritise phishing simulation programmes, mandatory reporting culture training, and validated IT/OT network segmentation audits.

Source: Marine Link | Date: 14.04.2026 | Credibility: High Additional sources: Smart Maritime Network

Test your response: Explore how insider behaviour and flat network architecture enable compromise in our stowaway tabletop →

Section 2: Regulations & Standards

[REGULATION] 6. IMO Maritime Cyber Code: 40+ states and organisations formally propose goal-based code at IMO — Safety4Sea

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

On 09.04.2026, a coalition of more than 40 flag states, port states, and international maritime organisations submitted a formal proposal to IMO calling for the development of a dedicated Maritime Cyber Code — a goal-based, binding (or semi-binding) instrument to establish minimum cybersecurity requirements for ships, ports, and the ship-shore interface. The proposal builds on the MSC.428(98) resolution framework but seeks to move beyond voluntary guidelines toward a structured code with defined compliance requirements. The submission follows the FAL 50 (March 2026) agreement to develop a non-mandatory code, suggesting a meaningful sub-group of IMO members favour a stronger instrument.

What this means: The scale of the coalition — 40+ states — signals strong political momentum for a binding or semi-binding maritime cyber framework; shipping companies and port operators should begin mapping current practices against MSC.428 now, as any resulting code is likely to crystallise these guidelines into formal requirements with audit and certification implications.

Source: Safety4Sea | Date: 09.04.2026 | Credibility: High

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

[REGULATION] 7. IACS Recommendation No. 194 — cyber security controls extended to the existing fleet — CCS / IACS

[Regulatory: IACS E26/E27] [Asset: Shipboard OT]

IACS published Recommendation No. 194 on 01.04.2026, providing a structured set of cybersecurity controls specifically designed for the existing trading fleet — a category explicitly excluded from the mandatory UR E26/E27 requirements that apply only to newbuildings with keel-laying dates on or after 01.07.2024. Rec 194 aligns its control framework with the NIST CSF five functions (Identify, Protect, Detect, Respond, Recover) and provides guidance that classification societies and operators can apply during periodic surveys and company SMS audits. The

publication directly addresses the "two-speed maritime cyber problem" where newer vessels are advancing toward structured compliance while the bulk of the operational global fleet — comprising tens of thousands of ships — remains without a comparable framework.

What this means: Fleet managers with mixed new/existing tonnage should treat IACS Rec 194 as an audit-ready baseline for their pre-2024 vessels; while currently non-mandatory, adoption ahead of potential regulatory escalation demonstrates due diligence and supports meaningful comparison of cyber posture across mixed-age fleets.

Source: IACS / CCS | Date: 01.04.2026 | Credibility: High

[REGULATION] 8. UK MCA MIN 732 (M+F) Amendment 1 — updated guidance for operations in conflict-affected and GNSS-degraded regions — UK MCA

[Regulatory: n/a (UK national)] [Asset: Shipboard OT | PNT/GNSS]

The UK Maritime and Coastguard Agency published Amendment 1 to Marine Information Note 732 (M+F) on 10.04.2026, updating practical guidance for shipowners, fishing vessel owners, seafarers, and fishers operating in conflict-affected regions. The amendment explicitly addresses GNSS interference as a navigational risk alongside physical security concerns, covering the Red Sea, Persian Gulf, and Strait of Hormuz operating environments. The guidance reinforces the use of independent position-fixing methods, recommends enhanced watchkeeping procedures, and advises operators to report GNSS anomalies to national and international monitoring bodies.

What this means: UK-flagged and UK-managed vessels transiting the Red Sea and Persian Gulf should treat MIN 732 Amendment 1 as a mandatory review item for their SMS and bridge standing orders; the explicit GNSS interference guidance is also a practical reference for operators under other flag states managing the same risk environment.

Source: UK MCA | Date: 10.04.2026 | Credibility: High

[REGULATION] 9. IMO approves Strategy on Maritime Digitalization — cybersecurity integration confirmed — Safety4Sea

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

In mid-April 2026, IMO formally approved its Strategy on Maritime Digitalization, confirming that cybersecurity is embedded as a cross-cutting requirement across all digitalization workstreams — covering autonomous shipping, data sharing, digital documentation, and connected port-ship interfaces. The strategy establishes a framework for how IMO member states and the maritime industry should approach technology adoption, with cybersecurity risk management treated as a prerequisite rather than a supplementary measure. The strategy directly informs the ongoing Maritime Cyber Code development work agreed at FAL 50.

What this means: The Digitalization Strategy signals that future IMO instruments — including the emerging Cyber Code — will be structurally aligned rather than issued as standalone amendments; operators investing in digital transformation should ensure their cybersecurity architecture is being designed alongside, not retrofitted into, digitalisation programmes.

Source: Safety4Sea | Date: mid-April 2026 | Credibility: High

---

Section 3: OT/ICS Threats & GNSS/PNT

[OT] 10. CISA ICS advisories — Siemens SICAM 8 and Hitachi Energy Ellipse: critical port-side energy management vulnerabilities — CISA

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

[HIGH] CISA published critical ICS security advisories on 02.04.2026 covering Siemens SICAM 8 (energy management platform used in substation automation) and Hitachi Energy Ellipse (asset management system for electrical infrastructure). Both products are deployed in port-side power infrastructure including shore power systems, crane electrical feeds, and terminal substation management. The advisories document vulnerabilities that could allow remote attackers to manipulate or disrupt energy management systems, with potential for cascading effects on operational continuity across connected terminal equipment.

What this means: Port operators and terminal managers running Siemens SICAM 8 or Hitachi Energy Ellipse in their electrical infrastructure should immediately assess patch status and apply vendor mitigations; given the role these systems play in crane power supply and terminal operations, exploitation could translate directly into cargo handling stoppages.

Source: CISA | Date: 02.04.2026 | Credibility: High

Test your response: Test your response to an OT attack targeting safety-critical port infrastructure →

[VULNERABILITY] 11. Fortinet FortiClient EMS critical RCE — CVE-2026-35616, unauthenticated, active exploitation reported — Fortinet PSIRT

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

[CRITICAL] Fortinet disclosed CVE-2026-35616 on 10.04.2026: an unauthenticated remote code execution vulnerability in FortiClient EMS (Enterprise Management Server), the endpoint management platform used widely by maritime security teams to manage fleet remote access endpoints, crew device policies, and VPN infrastructure. Active exploitation was confirmed in the advisory. Fortinet FortiClient is deployed across major shipping lines, classification societies, and port operators for centralised fleet endpoint management and remote connectivity — making this a high-value target for initial access brokers and ransomware affiliates seeking maritime corporate network footholds.

What this means: Maritime security teams running FortiClient EMS should treat CVE-2026-35616 as an emergency patch priority given confirmed active exploitation; until patched, consider isolating EMS management interfaces from internet-facing exposure and reviewing recent connection logs for anomalous EMS activity.

Source: Fortinet PSIRT | Date: 10.04.2026 | Credibility: High

---

[VULNERABILITY] 12. nginx-ui critical unauthenticated server access — CVE-2026-33032 (CVSS 9.8) — Security Affairs

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

[CRITICAL] CVE-2026-33032 was published on 15.04.2026, disclosing a critical vulnerability (CVSS 9.8) in nginx-ui — the widely used web-based administration interface for NGINX servers — allowing unauthenticated attackers to restart services, create, modify, and delete NGINX configurations, and gain effective server control. The vulnerability affects maritime logistics portals, fleet management web platforms, port community systems, and cargo documentation servers running NGINX with nginx-ui enabled. Exploitation requires no credentials and no prior access, making it trivially weaponisable in automated scanning campaigns.

What this means: Fleet IT teams and port web platform administrators should audit all NGINX deployments for nginx-ui exposure immediately; internet-facing instances should be patched or the management interface restricted to trusted internal networks pending patch availability — unauthenticated server-level access to maritime logistics infrastructure creates direct risk of service disruption and data exfiltration.

Source: Security Affairs | Date: 15.04.2026 | Credibility: High

---

[GNSS] 13. UK P&I Club: GNSS disruption advisory for bridge teams — Persian Gulf, Red Sea, Black Sea, Baltic, Eastern Mediterranean all flagged — UK P&I Club

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

[HIGH] The UK P&I Club published a dedicated GNSS disruption advisory for bridge teams on 14.04.2026, documenting persistent and simultaneous GNSS interference across six distinct maritime regions: the Persian Gulf, the Strait of Hormuz, the Red Sea, the Black Sea, the Baltic Sea, and the Eastern Mediterranean. The advisory notes that the geographic spread now encompasses the primary routes for European, Middle Eastern, and Asian trade, and that interference characteristics — including spoofed positions appearing at airports and inland sites — match patterns seen in coordinated electronic warfare operations. The club provides practical bridge guidance on identifying disruption, cross-checking position by alternative means, and reporting obligations.

What this means: The UK P&I advisory reinforces that GNSS interference is no longer a regional or theatrespecific risk — with six major trade corridors affected simultaneously, fleet operators must treat multi-source PNT cross-checking as a standing bridge procedure across the majority of global trade routes rather than a contingency measure for specific passages.

Source: UK P&I Club | Date: 14.04.2026 | Credibility: High

Test your response: Practice bridge team decision-making under GPS spoofing conditions in our free tabletop exercise →

Section 4: Ports & Supply Chain

[REPORT] 14. Marlink Cyber Intelligence Report: human error drives maritime cyber risk as crew networks become primary attack surface — Marine Link

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

The Marlink Cyber Intelligence Report released on 14.04.2026 provides the most comprehensive public baseline of maritime cyber threat activity for 2025, drawing on telemetry from across Marlink's managed maritime network. Beyond the headline incident count (covered in Section 1, Item 5), the report identifies structural vulnerabilities in how vessels and their operators manage the boundary between crew welfare networks and operational technology: in cases where IT/OT segmentation is absent or incomplete, phishing-enabled credential theft in the crew zone has been observed as a precursor to OT lateral movement. The report also notes that incident response maturity varies dramatically across vessel types and operator size, with smaller operators and tramping fleets showing the largest gaps.

What this means: Port and terminal operators procuring shipping services should consider including minimum cyber assurance requirements in their vendor qualification processes — the Marlink data confirms that crew network compromise is a realistic pathway to broader operational disruption, and the risk does not stay confined to the vessel.

Source: Marine Link | Date: 14.04.2026 | Credibility: High Additional sources: Smart Maritime Network

---

Section 5: People, Training & Governance

[GOVERNANCE] 15. ABS publishes "Human Readiness Levels for the Maritime Industry" whitepaper — crew-autonomy teaming cyber implications — ABS

[Regulatory: ABS Class] [Asset: Shipboard OT | Corporate IT]

ABS published its "Human Readiness Levels for the Maritime Industry" whitepaper on 13.04.2026, establishing a standardised framework for assessing crew preparedness in human-autonomy teaming (HAT) environments — vessels where autonomous or semi-autonomous systems increasingly share decision-making responsibility with human operators. The whitepaper identifies the human element as a critical cybersecurity vulnerability in contexts where crews may override, misinterpret, or fail to question outputs from compromised or manipulated autonomous systems. As cyber attacks targeting navigation and automation systems become more sophisticated, the framework provides a methodology for evaluating whether crew training and procedures are adequate to detect and respond to anomalous system behaviour.

What this means: Fleet managers investing in autonomous or AI-assisted bridge systems should incorporate the ABS Human Readiness Levels framework into their crew training and competency assessment programmes — effective cyber resilience in automated environments requires crews who understand the human-machine interface well enough to recognise when the machine is behaving under adversarial influence.

Source: ABS | Date: 13.04.2026 | Credibility: High

[REPORT] 16. CyberCube H1 2026 Global Threat Briefing: agentic AI transforms cyber underwriting model for marine insurers — CyberCube

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

CyberCube released its H1 2026 Global Threat Briefing on 13.04.2026, titled "AI Risk Landscape: Implications for Cyber (Re)insurance." The report identifies the emergence of "agentic AI" — autonomous AI systems capable of planning and executing multi-stage attacks with minimal human oversight — as requiring a fundamental shift in how cyber risk is modelled and underwritten. For the marine cyber insurance market, the implications are significant: automated reconnaissance and exploitation tools operating at AI speeds compress the window between initial access and claim-level damage, while AI-assisted phishing campaigns increase the effectiveness of the human-vector attacks that Marlink's data confirms dominate maritime incident reporting.

What this means: Marine underwriters and P&I clubs should begin incorporating agentic AI attack velocity assumptions into their exposure models; vessel operators seeking cyber coverage should expect increased scrutiny of AI-exposed surfaces — including autonomous navigation interfaces, AI-assisted cargo optimisation platforms, and fleet management APIs — during underwriting reviews.

Source: CyberCube | Date: 13.04.2026 | Credibility: High

Section 6: Upcoming Maritime Cyber Events

Maritime Cyber Security Conference 2026 — Manila | 15–16.04.2026 | Manila, Philippines Two-day conference: Day 1 leadership track on regulation, collaboration, evolving threats; Day 2 workshops for practitioners and vessel officers. Theme: "Access Granted: Anchors Up, Firewalls On." Link

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. Hosts "Marine CyberSafe" forum and showcases Maritime Cyber Assurance and Operations Centre. 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. Research on Cyber-Physical Systems — hacks on ECDIS, AIS, 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. 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

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

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

Recent Events — March–April 2026

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

IRClass Maritime Cyber Risk Management Training (10.04.2026, Online, India)
Classification-society-backed training for shipowners, managers, ports and terminals. IMO and IACS E26/E27 aligned curriculum. Link

4th Annual Maritime Cyber Safety Summit (13.04.2026, Miami Beach Convention Center, USA)
Invitation-only summit co-hosted by Carnival, Royal Caribbean, and NCL. Focus on OT cybersecurity for cruise vessels. Co-located with Seatrade Cruise Global. Link

World Border Security Congress (14–16.04.2026, Vienna, Austria)
High relevance for Port Facility Security Officers (PFSO) — biometric data protection, border/port security convergence. Link

Smart Maritime Network Rotterdam (15.04.2026, Rotterdam, Netherlands)
Port Community Systems (PCS) security: incident response for port digital infrastructure and cascade risk of PCS compromise. Link

---

Report compiled: 15.04.2026 | Coverage period: 01.04–15.04.2026 | Sources: 26 unique sources across Tier 1–4