

European Maritime
Safety Report
The Japan Association
of Marine Safety
London Research Office

Berlin Cathedral, rising majestically on the banks of the River Spree in Berlin, Germany

Supported by  日本 財団 THE NIPPON FOUNDATION

Article Summaries

26-25-1. Launch of a Public–Private Alliance under the EU Industrial Maritime Strategy

- A framework for public–private cooperation has been launched to implement the EU Industrial Maritime Strategy, published in March.
- On 2 September, the European Commission formally launched the EU Industrial Maritime Value Chains Alliance (EMA) and opened a call for applications.
- The Alliance will foster cooperation among shipyards, shipping companies, Member States, investors and others, with the aim of expanding manufacturing within the EU.

26-25-2. The EU’s Crisis Response to Mass Illegal Arrivals

- To prepare for situations such as the weaponisation of migration, the European Commission announced plans to establish an emergency response framework and to strengthen Frontex.
- Following mass arrivals in Ceuta, the Commission decided to provide Spain with €114.7 million in emergency assistance.
- In the English Channel, Frontex deployed a patrol vessel for the first time to support French search and rescue operations.

26-25-3. UK MAIB Interim Report on a Collision between a Crewed and an Unmanned Vessel

- The UK’s Marine Accident Investigation Branch (MAIB) published an interim report on a collision between a crew transfer vessel and an unmanned surface vessel.
- The crewed vessel was damaged and took on water, while the unmanned vessel sank. The causes and other findings are expected to be set out in the final report.
- The MAIB regards the investigation as important for examining how crewed and unmanned vessels can operate safely in the same waters.

26-25-4. Cyber Attacks Targeting Ships and Cyber Risk Management

- The Liberia Maritime Authority published details of a malware attack on a Liberian-flagged tanker.
- Eight of the 11 PCs on board were infected. Network segregation prevented the infection from spreading to navigation and machinery systems, and the vessel continued operating.
- The Authority updated its guidance on cyber risk management in safety management systems (SMS) and recommended measures such as network segregation.

(End of article summaries)

Full Articles

[26-25-1. Launch of a Public–Private Alliance under the EU Industrial Maritime Strategy](#)

In early September, the EU launched a framework for cooperation and coordination among public and private stakeholders to implement the EU Industrial Maritime Strategy, published in March. The Strategy aims to strengthen the competitiveness and economic security of Europe's maritime industry and is structured around six pillars. Under its first pillar, 'Build, Equip and Repair', the Strategy had set out plans to establish the EU Industrial Maritime Value Chains Alliance (EMA) to strengthen Europe's capacity to manufacture ships and maritime equipment. [\[1-1\]](#) [\[1-2\]](#)

As a concrete step, on 2 September the European Commission formally launched the EMA and opened a call for applications. The Alliance brings together public and private stakeholders, including shipbuilders and maritime equipment manufacturers, users such as shipping companies, Member States and regions, investors and research institutions. Its priority areas are: (1) decarbonised vessels for short-sea, coastal and inland waterway transport; (2) special-purpose vessels and workboats, such as icebreakers; (3) ocean observation equipment, such as surface and underwater drones; (4) net-zero technologies, such as clean propulsion; (5) smart and sustainable manufacturing processes; and (6) ship recycling. In these areas, the Alliance will identify demand, production capacity and supply chain challenges, and will work towards scaling up manufacturing and deployment within Europe, developing strategic projects, and aligning the investment priorities of the EU and its Member States. [\[1-3\]](#) [\[1-4\]](#) [\[1-5\]](#)

Underlying this initiative is the intensification of international competition facing the European maritime industry. The EU has noted that, although European shipbuilding is strong in high-value and specialised vessels, it faces fierce competition. Among the factors it cites are large-scale support from the governments of third countries (non-EU countries) for their own shipbuilding industries and sales at unfairly low prices. In light of this situation, the Council of the European Union also supported the launch of the EMA on 8 June and encouraged its rapid establishment. [\[1-2\]](#) [\[1-6\]](#) [\[1-7\]](#)

Participation in the EMA is subject to certain conditions. Eligible participants include companies, industry associations, public bodies, investors and research institutions active in the EU. Entities established outside the European Economic Area (EEA) are assessed on a case-by-case basis. A mechanism also allows the participation of entities controlled by third countries to be restricted in discussions on strategically important matters. The call will remain open on a rolling basis, with the first cut-off date set for 16 October. [\[1-3\]](#) [\[1-5\]](#)

Attention will now turn to the specific investments that public–private cooperation through the EMA may generate in scaling up the manufacture of decarbonised vessels, workboats, ocean observation equipment and other products within Europe.

26-25-2. The EU's Crisis Response to Mass Illegal Arrivals

In September 2026, the EU announced a succession of measures to respond to crises involving mass illegal arrivals and to strengthen the European Border and Coast Guard Agency (Frontex). As reported in Issue No. 26-15 of this report, work to put in place a framework for tackling illegal migration has been progressing: in June, the Pact on Migration and Asylum began to apply and the EU Action Plan for the Channel route was presented. [\[2-1\]](#)

Against this background, on 16 September, European Commission President Ursula von der Leyen announced that the Commission would propose a new European Emergency Response Framework. The framework is intended for exceptional emergencies in which large-scale movements of people are deliberately engineered and used as an instrument of political pressure. In such cases, it would allow standard procedures to be made temporarily more flexible, subject to strict requirements. [\[2-2\]](#)

Subsequently, on 29 September, the European Commission published its '5-point plan to prevent, anticipate and respond to sudden, mass illegal arrivals'. The plan sets out five points: (1) strengthening cooperation with partner countries to prevent illegal migration; (2) reinforcing the EU's external borders; (3) improving the monitoring of migration trends and early warning; (4) dismantling migrant smuggling and human trafficking networks; and (5) strengthening the framework for effective return and readmission (whereby the countries concerned take back their own nationals). The plan also provides for a stronger role for Frontex, including the rapid deployment of staff and equipment in emergencies and support for returns. [\[2-3\]](#)

The plan was drawn up against the backdrop of the large-scale illegal border crossings into the Spanish territory of Ceuta at the end of July. On 30–31 July, approximately 72,000 people entered Ceuta illegally from Morocco, according to estimates by the Spanish authorities. In response, on 9 September the European Commission decided to grant Spain €114.7 million in emergency assistance. The funding will be used for purposes including border surveillance and security, the screening of migrants, reception and returns. In addition, at Spain's request, on-the-ground operational support from Frontex, the European Union Agency for Law Enforcement Cooperation (Europol) and the European Union Agency for Asylum (EUAA) was expanded. [\[2-4\]](#) [\[2-5\]](#)

Frontex activity has also been stepped up in the English Channel under the EU Action Plan published in June, which provided for the deployment of Frontex maritime and aerial surveillance assets. On 4 September, Frontex announced that it had deployed a patrol vessel to the Channel for the first time, in addition to the aerial surveillance it has conducted there since 2021. Working in tandem with a surveillance aircraft, the vessel detects and tracks small boats and passes this information to the French authorities, thereby supporting search and rescue operations. [\[2-6\]](#) [\[2-7\]](#)

26-25-3. UK MAIB Interim Report on a Collision between a Crewed and an Unmanned Vessel

On 17 September, the UK's Marine Accident Investigation Branch (MAIB) published an interim report on the collision between the crew transfer vessel (CTV) *Iceni Legend* and the unmanned surface vessel (USV) *X18*. The accident occurred on 19 September 2025 within the Greater Gabbard Offshore Wind Farm in the North Sea, approximately 25 nautical miles east of Felixstowe. In the UK, an interim report must be published where the final report cannot be published within 12 months of an accident, and this report was issued on that basis. [\[3-1\]](#) [\[3-2\]](#)

At 12:13 on 19 September 2025, *Iceni Legend* (length overall 22.4 m; six persons on board) was under way to transfer personnel to an offshore wind installation. It collided with *X18* (length 4.58 m; weight 840 kg), which was conducting an underwater survey. *Iceni Legend* sustained damage to its port bow and took on water, but returned to port under its own power, and no one was injured. *X18*, by contrast, was severely damaged and sank; as of the publication of the interim report, its wreckage had still not been recovered from the seabed. [\[3-2\]](#)

As this case involved an actual collision between a crewed and an unmanned vessel operating in the same waters, one of the central issues addressed by the investigation is likely to be how the two vessels perceived one another and how the collision occurred.

The MAIB's investigation examined, among other matters, (1) the environmental conditions on the day, (2) each vessel's awareness of, and ability to communicate with, the other, and (3) the regulatory framework for autonomous and unmanned vessels. The investigation has now been completed. A draft report will be circulated to stakeholders for a 30-day consultation before the final report is published. The final report is expected to set out the causes of the collision and the sequence of events leading up to it. [\[3-2\]](#) [\[3-3\]](#)

On 30 September, the MAIB also published its Annual Report 2025, which summarises its investigative activities over the year. The report highlights this case as an example of the challenges facing maritime safety in the years ahead. It notes that, although no one was harmed, the accident is providing an opportunity to understand how a remotely controlled, slow-moving unmanned vessel operates in the same waters as a fast vessel operated by a human crew. It further describes the investigation as an important one that will help inform consideration of standards for the construction and operation of vessels, seafarer training, and questions such as how humans anticipate the actions of machines and how machines anticipate those of humans. [\[3-3\]](#)

The interim report does not identify the causes of the collision. The key question going forward is what collision-prevention measures will be considered, in light of the findings of the final report, to support the safe operation of crewed and unmanned vessels in the same waters.

26-25-4. Cyber Attacks Targeting Ships and Cyber Risk Management

On 20 September, the Liberia Maritime Authority published details of a malware attack on a Liberian-flagged tanker. The attack took place on 8 August while the vessel was crossing the Atlantic bound for the United States. The Authority's investigation found that, before the attack, there had been repeated unauthorised remote access through the firewall of the vessel's satellite communications system, along with several other intrusion attempts. It is believed that an external attacker remotely gained access to the onboard systems and introduced malware, which then spread to the vessel's business network. Eight of the 11 PCs on board were infected. The server's operating system and data were deleted, as was the backup data. However, because the onboard networks were segregated, the malware was prevented from spreading to safety-critical systems such as navigation and machinery, and the vessel continued normal operations. [\[4-1\]](#)

Similar malware infections of shipboard networks have occurred before. In 2019, the United States Coast Guard (USCG) reported an incident in which malware significantly degraded the functionality of the onboard computer system of a large vessel bound for the Port of New York and New Jersey. In that case, too, the control systems essential to the vessel's operation were not affected. However, the USCG pointed out that the vessel had been operating without effective cyber security measures, leaving critical control systems exposed to significant vulnerabilities. It recommended measures such as network segregation. [\[4-2\]](#)

On 18 September, two days before publishing details of this incident, the Liberia Maritime Authority also updated its guidance on integrating cyber risk management into safety management systems (SMS). The guidance follows the International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management. It sets out measures built around six functions that are consistent with the US National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0: Govern, Identify, Protect, Detect, Respond and Recover. [\[4-3\]](#) [\[4-4\]](#)

According to the guidance, Liberian-flagged ships are required to address cyber risks in their SMS. Where they fail to do so, a deficiency may be raised during a port State control inspection. The ship may then be required to undergo an internal audit before departure, or may be detained until the deficiency has been rectified. In publishing details of the incident, the Authority also called for this guidance to be consulted. It stated that cyber attacks should be treated as seriously as physical attacks on ships. The Authority went on to recommend measures including (1) verifying that network segregation and access controls are functioning effectively, (2) strengthening the monitoring of remote connections, and (3) testing backup and recovery procedures and protecting them from unauthorised access. [\[4-1\]](#) [\[4-3\]](#)

Amid growing concerns over emerging threats, including cyber attacks that exploit artificial intelligence (AI), effective cyber risk management is important to help ships respond appropriately.

Yoshihiro Kawakami
Researcher, London Research Office
The Japan Association of Marine Safety