

Maritime Summary Note n°254 – October 2023

« Cybersecurity : a major challenge for the maritime sector »

The digital era represents major opportunities in terms of safety, economic performance, and environmental monitoring for the maritime sector. From navigation to propulsion, and from cargo management to maritime traffic control, the stakes are colossal. Cyberattacks are becoming increasingly common as the digitalization of our activities progresses. Known and uncorrected technical vulnerabilities, human vulnerabilities through a lack of awareness of cyber threats, or organizational vulnerabilities exist to varying degrees.

The interconnectivity of all stakeholders and the aggregation of services (smart ports, smart ships, smart containers, AI, etc.) increase the risk of cyberattack propagation (ransomware, malware). The impact can be digital, physical, financial, or legal, and can harm an entity's reputation. From now on, the safety of people, property, and the environment is also at stake. The world's three largest shipping companies—Maersk, MSC, and CMA CGM—have all fallen victim to cyberattacks in recent years. The maritime sector is becoming a playground for organized professional hackers whose resources continue to grow. Their techniques are increasingly sophisticated. Their motivations vary, including criminal gangs, political activists, foreign powers and state-sponsored actors, and terrorist groups—all the more so in the currently tense geopolitical context. How does the maritime world address these cyber threats?

Contextual Elements

Malicious codes and ransomware are the most frequent threats, ahead of direct network intrusions. The logistics and supply chain sector is the most heavily affected, ahead of individual shipping lines and port authorities. The United States and France rank as the two states that have suffered the highest number of reported maritime cyber incidents.

Shipboard Dimension

Cyber systems deployed on board commercial vessels or offshore energy platforms are strictly classified either as IT (Information Technology) or OT (Operational Technology).

IT can contain all kinds of non-operational data for the vessel's navigation, which are nonetheless important, such as the crew list, maintenance planning, work permits, electronic manuals and certificates, and the charter party. OT provides the underlying architecture for all the vessel's operational functions, including navigation, propulsion, and the steering gear. It encompasses information systems such as the GPS, the ECDIS (Electronic Chart Display and Information System), the SCADA (Supervisory Control and Data Acquisition) real-time monitoring system, and associated programmable logic controllers and interfaces to manage shipboard machinery, voyage data recorders, dynamic positioning, and vessel stability through ballast water management. A cyberattack targeting OT is liable to directly jeopardize the vessel and its crew.

Every shipowner seeks to optimize its shipping operations. Digital data analysis represents a powerful competitive advantage and drives all stakeholders to follow suit. Governments, regulatory bodies, and customer requirements concurrently push toward the paths of traceability and permanent control provided by digital tools.

In France, initial student training at the ENSM has integrated cybersecurity since 2019 through an awareness module covering regulations and maritime or port-specific attack scenarios (prevention, dissemination of best practices, etc.). Several students have participated in research projects involving the creation of cyber-crisis scenarios via the MARINS simulator and the securing of the S-100 standard (the new electronic navigational chart framework), thereby testing maritronics and the human element.

In partnership with the École Navale¹, ENSTA Bretagne, and IMT Atlantique, a specialized master's degree in the cybersecurity of maritime and port systems was established. It is regrettable that this program was not renewed this year.

Port Dimension

The revolution of "Ports 2.0" was achieved thanks to port digital service providers through the Cargo Community System (CCS) and the Port Community System (PCS). The CCS is a specialized software platform that facilitates the port transit of cargo and simplifies administrative workflows for industry professionals (shipowners, freight forwarders, shipping agents, terminal operators, port authorities, and customs).

The PCS is a digital solution that enables the planning and organization of vessel calls. A breach of the integrity or availability of a port's power management system (transformers, generators, and PMS) can trigger a power disruption or a blackout, bringing all port activity to a complete standstill. This includes IT and OT systems, the Vessel Traffic Services (VTS), lighthouses, locks, bridges, gantry cranes, refrigerated warehouses, reefer container monitoring, onshore power supply (OPS) for ships at berth, pumps, safety and security systems, access control, and automated gates. The automation of container cranes, along with sensors and cameras capable of adaptively analyzing behaviors, transit bottlenecks, and predictive maintenance, has henceforth become a concrete reality.

Maritime cybercrime and its operational patterns

The higher the connectivity of vessels and ports, the more aggressively the cyber threat evolves, manifesting as network blackouts, data breaches, cargo losses, bunkering fraud, phishing, GPS signal spoofing/jamming, malicious download of bills of lading, and container theft.

In 2011, the Port of Antwerp fell victim to a landmark cyberattack. That same year, the European Network and Information Security Agency (ENISA) published a warning report regarding the fragile state of digital security across the maritime cluster. In 2017, the global NotPetya cyberattack infected thousands of computers, disrupting multi-national corporations and critical infrastructures for months, including the monitoring computers of the Chernobyl nuclear site, the ports of Mumbai and Amsterdam, and the entire global logistics machinery of Maersk.

The cumulative cost of this single event was estimated to breach \$10 billion. Although this global cyberattack triggered a heightened awareness of digital vulnerabilities, the threat is today more present than ever. According to Allianz's Safety and Shipping Review, the current diagnostic is deeply worrying: 44% of maritime professionals have faced a cyberattack over the past three years, and one-third of shipping organizations completely lack a dedicated cyber plan (such as a Disaster Recovery Plan or a Business Continuity Plan).

Furthermore, four out of ten professionals estimate that their entity under-invests capital to counter the cyber threat. Because a cyberattack relies fundamentally on detecting and exploiting a victim's technical and human gaps, it is imperative to reinforce the "frontline" actors of this shadow war. This applies not only to the CISO (Chief Information Security Officer / RSSI) functions—most of which are already constantly battling these incursions—but must stem directly from executive boards (directions générales). They alone command the institutional power to grant Chief Information Officers (CIOs / DSI) financial resources matching the scale of the threat, while compelling all end-users and operators to strictly integrate cybersecurity into their daily workflows.

Regulatory frameworks and international mandates

The international tier and IMO resolutions

The cyber risk historically remained within the blind spot of international maritime law, subject only to highly generalized voluntary recommendations from the IMO. For instance, the ISPS Code (International Ship and Port Facility Security Code)—the global benchmark treaty governing maritime security—

¹ The **École Navale** (French Naval Academy) operates a specialized maritime cybersecurity research and training simulator (maritime cyber range), managed by the Cyber Defense of Naval Systems Chair.

merely states within its non-mandatory Part B that: "the ship security assessment should address (...) radio and telecommunication systems, including computer systems and networks."

Acute to these compounding vulnerabilities, the IMO, through its Maritime Safety Committee (MSC), formally adopted Resolution MSC 428(98) in June 2017, entitled "Maritime Cyber Risk Management in Safety Management Systems". While this text recognizes the urgent necessity to raise awareness across the global fleet, it remains highly generalized and shifts the responsibility of defining explicit enforcement conditions onto individual Member States. Crucially, this resolution is legally adoped to the International Safety Management Code (ISM Code). It is precisely through this safety management audit framework that ocean carriers' digital resilience is audited and verified.

Concurrently, the IMO published high-level guidelines on maritime cyber risk management in 2016 and 2017², structured around five core functional steps:

1. Identify: Clearly define personnel roles and their specific responsibilities regarding cyber risk management, while mapping out sensitive shipboard systems and critical datasets.
2. Protect: Implement risk control processes, data encryption, emergency contingency plans, and secure the continuous continuity of operations.
3. Detect: Develop and deploy the necessary technical monitoring activities to instantly detect a cyber event or network anomaly.
4. Respond: Execute a pre-engineered response plan to cultivate operational resilience and rapidly isolate infected networks.
5. Recover: Identify and deploy systematic backup measures to successfully restore all corrupted maritime systems to safety.

These circulars concurrently refer to the comprehensive guidelines issued by sovereign States, flag administrations, and professional maritime sector organizations. Indeed, in parallel with the IMO's workflows, international maritime associations, ocean carrier representatives (CLIA, INTERTANKO, INTERCARGO, BIMCO), classification societies operating through the IACS (International Association of Classification Societies), marine underwriters³, and state administrations such as the USCG (U.S. Coast Guard) publish their own cyber hygiene handbooks. These frameworks detail secure network architectures, access control, data protection, and incident assessment and response protocols.

The International Organization for Standardization (ISO) commands a series of standards that successfully complement maritime cybersecurity workflows, notably:

- ISO 28000: governing security management systems for the supply chain.
- ISO 24060: (Ships and marine technology — Ship software logging system for operational technology), specifically tailored for onboard OT tracking.
- ISO/IEC 27001: (International standard for information security management systems — ISMSs), which stands as the most globally recognized benchmark framework for the continuous improvement of an information security management system.

The IACS issues technical recommendations, selected of which have been formalized into mandatory Unified Requirements (UR) binding upon all IACS member classification societies. This regulatory mechanism contributes to guaranteeing that greenfield newbuild vessels strictly comply with the latest cybersecurity benchmarks from the design phase, though each individual member remains free to enforce even more stringent conditions.

These joint workflows successfully homogenize certification baselines regarding the cyber-resilience of vessels and the cybersecurity of shipboard embedded systems and equipment, driven by the implementation of UR E22, UR E26, and UR E27. The international standardization of cybersecurity and its systemic integration into ship system engineering remain fundamental.

The European tier and community directives

At the regional tier, the European Directive (EU) 2016/1148 on the Security of Network and Information Systems (NIS Directive), which entered into force in 2018, established the very first European regulatory framework designed to ensure a "high common level of security of network and information systems across the EU" across all motorized transport modes.

² Revised MSC Circular 1526 of 1 June 2016 'Guidelines on maritime cyber management' and MSC.1-FAL.1/Circ.3.

³ "guide to cyber – risk: managing the impact of increasing inter connectivity" publié par Allianz Global Corporate & Speciality (AGCS) sept 2015.

Statutory obligations are henceforth addressed to Member States and critical operators alike to guarantee a unified, synchronized European response to global cyber threats.

The revised NIS 2 Directive of 2022⁴ mandates that Member States must be positioned to respond to network and information system security incidents through the creation of a competent national authority. Member States are required to cooperate and exchange real-time intelligence regarding ongoing cyber threats. They must cultivate a robust security culture across the vital sectors of the economy that depend heavily on ICT, such as energy, transport, water management, banking, financial markets, healthcare, and digital infrastructure. Corporations identified by Member States as Essential or Important Entities (EE/EI — Entités Essentielles / Entités Importantes) within these critical sectors will be legally required to implement appropriate technical and organizational security measures while reporting serious incidents to the competent national authorities.

Shipping companies and port terminal managers are strictly subject to these statutory provisions. Technical and organizational measures—strongly embedding the human factor element—operate as the primary levers of action for maritime cybersecurity. This overhauled, highly demanding iteration must be transposed into domestic national legislation by late 2024 at the latest. It enforces severe penalties for regulated entities, ranging from heavy financial fines to the absolute withdrawal of their operating license in the event of non-compliance with NIS 2.

This regulatory mandate compels EE/EIs to invest capital while establishing a level playing field across the market. Furthermore, these critical operators are held legally accountable for the cybersecurity of their third-party contractors and their entire supply chain, generating a powerful contractual impact.

The directive makes it mandatory to report a cyber incident within a strict 24-hour window, aiming to foster synchronized information sharing among Member States and better determine whether a digital event carries cross-border ripples. It is only by sharing threat intelligence and operational experiences that the industry will successfully forge robust standards and cybersecurity best practices. Within this framework, France Cyber Maritime (hosting the maritime M-CERT) maintains ADMIRAL, a public centralized database compiling known and public cybersecurity incidents that have targeted the wider maritime and port sectors on an international scale.

The French domestic framework and military planning

Within the French landscape, the Military Planning Law (Loi de Programmation Militaire — LPM) operates as the master strategic defense blueprint, voted every five years. It officially designates approximately 250 Operators of Vital Importance (OIV — Opérateurs d'Importance Vitale), encompassing both private corporations and public entities deemed indispensable to the continuous survival and functioning of the Nation. These OIVs are bound by strict statutory legal obligations regarding infrastructure cybersecurity.

Domestic French regulations integrate the specific mandates of the ISPS Code within Division 130, annexed to the Decree of November 23, 1987 (as amended) relating to ship safety and pollution prevention. Article 130.28 explicitly decrees for vessels:

"III. Integration of Cyber Risk: Any company mandated to hold a Document of Compliance shall ensure that cyber risks are appropriately incorporated into its Safety Management System (SMS). During audits conducted for the issuance or renewal of the Document of Compliance, and in accordance with IMO Resolution MSC 428(98), the company shall expose, at a minimum, the measures implemented regarding:

- a) Its general cybersecurity policy;
- b) The execution and updating of its risk assessment, including an inventory of existing systems and procedures;
- c) The technical, human, and organizational procedures put in place;
- d) Daily monitoring and follow-up protocols;
- e) Alert and crisis management procedures."

Just as with compliance tracking for safety, security, environmental, and social standards, cybersecurity now falls under the direct jurisdiction of the Ship Safety Centers (Centres de Sécurité des Navires — CSN). Pursuant to Resolution MSC 428(98), inspectors currently only audit the corporate headquarters of shipping lines. A structural lack of resources, time, and specialized expertise severely limits the flag

⁴ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022.

administration's capacity to perform granular, highly precise technical assessments of these cyber systems.

Facing these threats, the relevant public administrations—the General Secretariat for the Sea (SGMer), the Directorate General for Maritime Affairs, Fisheries and Aquaculture (DGAMPA), and the Directorate General for Infrastructure, Transport and Mobility (DGITM), alongside the National Cybersecurity Agency of France (ANSSI)—the maritime/port sector, and the cybersecurity industry organized themselves by founding the Maritime Cyber Council (C2M2 — Conseil Cyber du Monde Maritime) in 2019.

The council's workflows followed two core directions: first, a macro-analysis of risks and potential attack scenarios to identify systemic vulnerabilities and prioritize action plans; second, the adoption in 2021 of a comprehensive Maritime Cyber Strategy pinning down these actions. Backed by ANSSI and driven by the impulse of SGMer, the France Cyber Maritime association was established in 2020 to forge deep synergies between the maritime cluster and the cybersecurity world.

The association provides specialized cybersecurity expertise and live emergency assistance during active incidents, thereby significantly strengthening the resilience of the sector. France Cyber Maritime operates the M-CERT (Maritime Computer Emergency Response Team), a national center dedicated to monitoring, analyzing, and sharing anonymized threat intelligence, vulnerabilities, and incidents targeting the maritime and port grids. Structurally, the association is articulated around three colleges: public actors (State agencies, ministries, regional collectivities), users (shipowners, ports, commercial fisheries), and solution providers (hardware, technical auditing, specialized underwriting). Cultivating a deep cyber risk awareness (acculturation) remains fundamental both ashore and at sea. As with legacy marine risks, the overriding logic centers on reinforcing prevention through long-term technical and human capital investments, while covering residual liabilities through specialized corporate insurance.

Cyber risk underwriting and marine insurance

A structural logic of absolute cyber risk exclusion historically characterized traditional marine insurance policies on the international market. To meet changing commercial requirements, the cyber-insurance sector expanded aggressively over recent years through dedicated, standalone policies—even though these frameworks initially generated severe underwriting losses for insurers. In 2020, underwriters collected €130 million in premiums against a monumental €250 million in covered claims.

This digital risk remains exceptionally complex to assess, both in its volatile form and its cascading economic repercussions—most notably regarding business interruption losses and revenue deficits resulting from operational blackouts. This exposure has triggered a sharp tightening of risk selection criteria, coupled with the application of steep premium surcharges and elevated deductible (franchise) baselines. In 2020, for every €1 of premium paid, €10 of liabilities were covered by cyber underwriters. Because cyber-insurance remains a developing product, no unified market standard exists today. It is structurally structured around four core pillars:

1. Prevention: pre-incident vulnerability assessments and technical penetration testing.
2. Assistance: immediate dispatch of cyber-forensics systems experts, specialized legal advisors, and crisis communication experts.
3. Operations Coverage: absorbing business interruption financial losses and operational deficits.
4. Liability Coverage: covering third-party lawsuits, regulatory fines, and legal defense costs.

The insurance policy must be surgically adjusted to the specific operational footprint of the entity, rendering the use of a specialized marine broker essential to benchmark competing market offers.

Ultimately, the defining question for the industry is no longer how or when a cyberattack will strike, but rather: will my organization display enough resilience to withstand and recover from it? The stakes of cybersecurity are permanent and pressing. The rapid rise of Artificial Intelligence, maritime surveillance drones, and unmanned autonomous vessels will profoundly alter tomorrow's operational workflows and international maritime law alike.

Camille VALERO

With the support of the DGAMPA, France Cyber Maritime, and Bessé Insurance Brokers.

English translation generated by Gemini AI