

MARITIME CYBER THREAT OVERVIEW 2025

IN COLLABORATION WITH

Alcyconie · ATOS · BZHunt · DIATEAM · FMES · Glimps · Marlink · Orange Cyberdefense · Semsoft (LESTR) · XRATOR

UNDER THE EUROPEAN PROJECT

SAFEDIGIMAR

FOR A SAFER DIGITAL MARITIME EUROPE

Co-funded by
the European Union

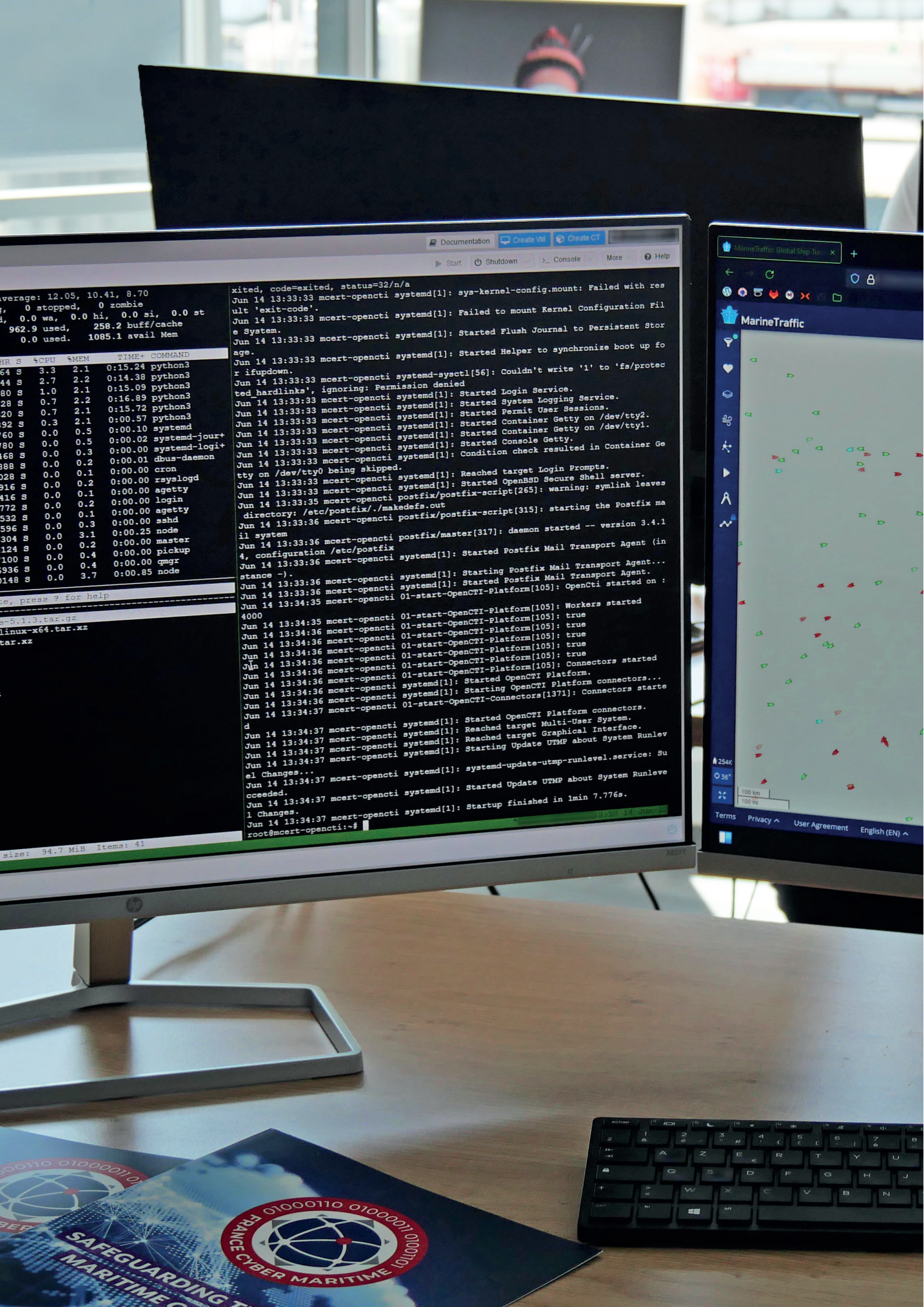

Documentation
Create VM
Create CT
Start
Shutdown
Console
More
Help
MarineTraffic
SAFEGUARDING
MARITIME
FRANCE CYBER MARITIME
01000110 01000011 01001101

TABLE OF CONTENTS

FOREWORDS 2

ABOUT THIS REPORT 3

2025 IN FIGURES 4

THE GEOPOLITICAL BACKDROP 8
Contribution from FMES

TWO THREATS, ONE NAME: REFRAMING 2025'S MARITIME INCIDENTS 11
Contribution from XRATOR

PORT SECTOR SPOTLIGHT: REHEARSING THE ATTACKER'S PLAYBOOK 13
Contribution from DIATEAM

OT SYSTEMS IN THE EYE OF THE STORM
Contribution from Orange Cyberdefense 15

THE SEA-SHORE LINK: A NEW FRONTIER
Contribution from Marlink 18

SPOTLIGHT: AIS SPOOFING — FROM DISAPPEARANCE TO DECEPTION
Contribution from Semsoft (LESTR) 21

MAJOR VULNERABILITIES EXPLOITED IN 2025, AND TRENDS
Contribution from GLIMPS 24

WHEN THE TIDE TURNS: AI-DRIVEN CYBERATTACKS AND WHAT THE MARITIME SECTOR MUST WATCH FOR
Contribution from BZHunt 27

AI BECOMES A STRATEGIC ACTOR IN THE INFORMATION CONFLICT
Contribution from ATOS 30

BUILDING OPERATIONAL RESILIENCE IN AN ERA OF HYBRID RISKS
Contribution from ALCYCONIE 33

CONTRIBUTORS TO THIS EDITION 37

Reproduction, distribution, and commercial use prohibited without written authorization from France Cyber Maritime.

FOREWORD

FROM THE DIRECTOR OF FRANCE CYBER MARITIME



The maritime, port and inland waterway sector plays a vital role in our economies and strategic balance. It underpins trade, supply chains and industrial activity.

The year 2025 confirms that the threat to our ecosystem is no longer peripheral or theoretical. It is intensifying as geopolitical tensions, organized crime, hacktivism, and the digitization of operations reinforce one another. M-CERT recorded 936 incidents affecting the maritime sector worldwide in 2025, compared to 604 in 2024—a 55% increase. Behind these figures lie service outages, data breaches, extortion, disruptions to navigation, and vulnerabilities among subcontractors.

This overview highlights a multifaceted threat. Denial-of-service attacks, often carried out by hacktivist groups, remain numerous. But the rise of cybercriminal tactics—particularly data breaches and double extortion—calls for heightened vigilance. Navigation systems, sea-to-land links, port infrastructure, industrial environments, and digital or satellite service providers are becoming key risk areas.

The unique nature of the maritime sector lies in the interdependence between information systems and physical operations, as well as between safety and security. A cyber attack can affect the ability to load or unload cargo, to navigate and locate vessels, as well as to communicate or plan operations. Maritime cybersecurity therefore requires a detailed understanding of the specific industries, operational constraints and interdependencies particular to the sea and ports.

The response must remain pragmatic. Artificial intelligence and offensive automation enhance certain adversarial capabilities, but the fundamentals remain the same: understanding one's digital assets, mapping dependencies, securing access, patching vulnerabilities, preparing for degraded operations, training teams, and organizing incident response.

Against this backdrop, France Cyber Maritime, through its members and M-CERT, aims to contribute to a shared understanding of the threat, without fuelling anxiety. The aim is to provide stakeholders in the maritime and cyber sectors with useful information to enable them to take action. The sector's resilience will depend on our collective ability to cooperate, share early warning signs and learn from incidents.

I would like to thank the contributors to this edition. Their analyses demonstrate the maturity of a committed maritime cybersecurity community. Now more than ever, cybersecurity is essential to maintaining trust and ensuring the sector's continuity.

Christian CÉVAËR

ABOUT THIS REPORT



ABOUT FRANCE CYBER MARITIME AND THE M-CERT

France Cyber Maritime is a non-profit association (Loi 1901) whose mission is to strengthen the cybersecurity of the French maritime and port sector. It brings together public bodies, maritime and port operators, and qualified cybersecurity solution providers.

France Cyber Maritime's objectives are to develop a network of maritime cybersecurity expertise by encouraging the creation of high-value services suited to the industry's needs, and to improve the resilience of maritime and port operations against cyber threats by operating the M-CERT (Maritime Computer Emergency Response Team), which provides information and assistance to the sector.

Since March 2021, the M-CERT has monitored and analysed the threat facing the maritime world and produces regular analysis bulletins for the association's members, in addition to risk-prevention, alerting and incident-response coordination services, working alongside State authorities and other cybersecurity organisations.

ABOUT SAFEDIGIMAR

End of 2025, the European Commission officially signed a grant agreement with a consortium including France Cyber Maritime, FEPORT and the Italian Maritime Cluster / Federazione del Mare following their successful application to the call for proposals on the SAFEDIGIMAR project. The project, which has been awarded as part of the Digital Europe programme promotes the implementation of NIS2 related measures and will develop tailor-made solutions to strengthen the cybersecurity posture of the ecosystem. The project monitors risks and threats impacting the sector, disseminates good practices while assisting victims of cyberattacks from the maritime community.

METHODOLOGY

Identifying the cybersecurity incidents affecting the maritime world presented in this report required daily monitoring of a range of specialised websites and dedicated social media feeds, complemented by technical sensors gathering additional data. Information judged relevant was characterised against a set of criteria, then analysed and capitalised by M-CERT analysts.

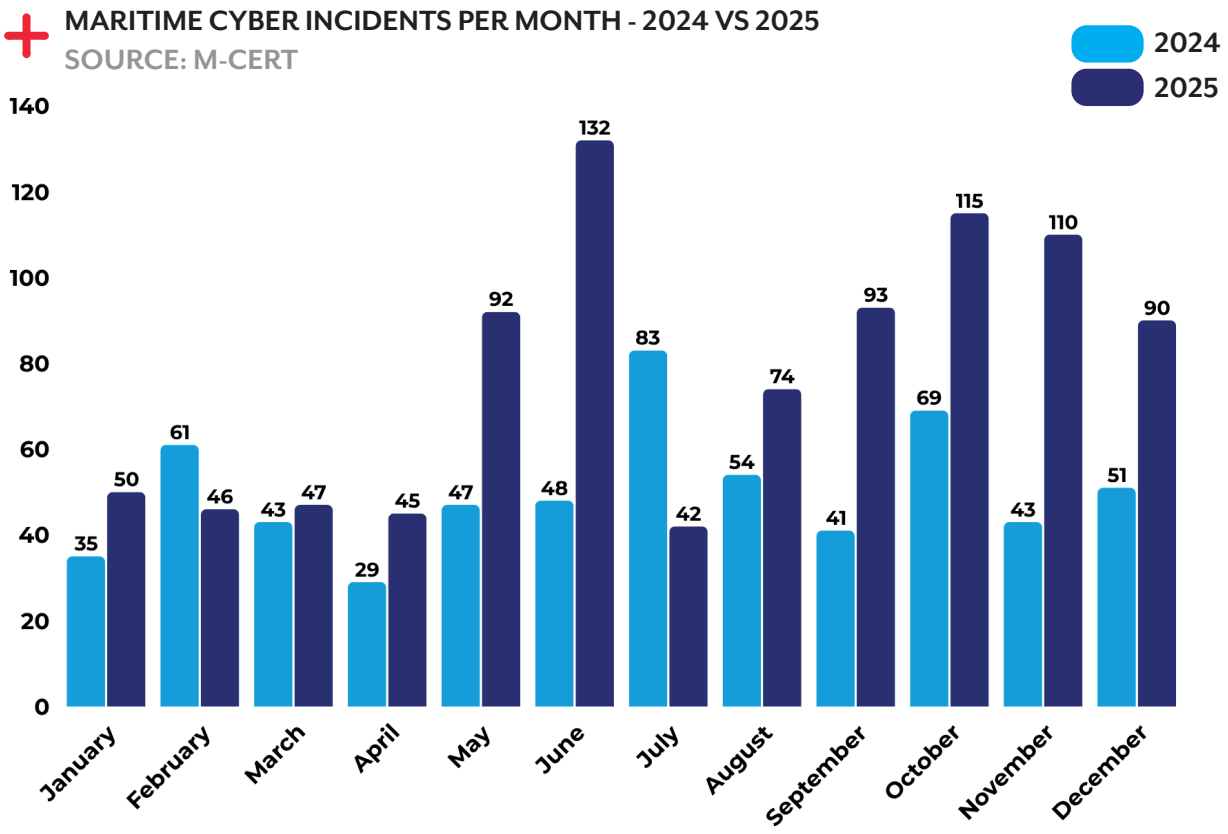
For this 2025 edition, M-CERT's own incident tracking and statistics are complemented by written contributions from partner organisations across the maritime cybersecurity ecosystem — Alcyconie, ATOS, BZHunt, DIATEAM, FMES, GLIMPS, Marlink, Orange Cyberdefense, Semsoft (LESTR) and XRATOR. Each section is attributed to its contributing organisation and reflects that organisation's own analysis and views.

1.

2025 IN FIGURES

M-CERT recorded the following cybersecurity incidents affecting the maritime sector worldwide in 2024 and 2025 (no victim names disclosed).

METRIC	2024	2025
Incidents recorded	604	936 (+55%)
Average incidents / month	50.3	78.0
Countries targeted	70	82 (90+ combined)
DDoS share of incidents	55.3%	51.6%
Ransomware share of incidents	33.0%	26.1%
Data-leak share of incidents	7.3% (44)	17.2% (161, +266%)
Hacktivism share (actor type)	61.3%	53.4%
Cybercrime share (actor type)	36.9%	44.7%
State-sponsored incidents (count)	2	2
Top targeted sector	Port activity - 174 incidents	NA



ATTACK TYPES AND THREAT ACTORS

CATEGORY	2024	2025
DDoS	334	483
Ransomware	199	244
Data leak	44	161
Other	27	48

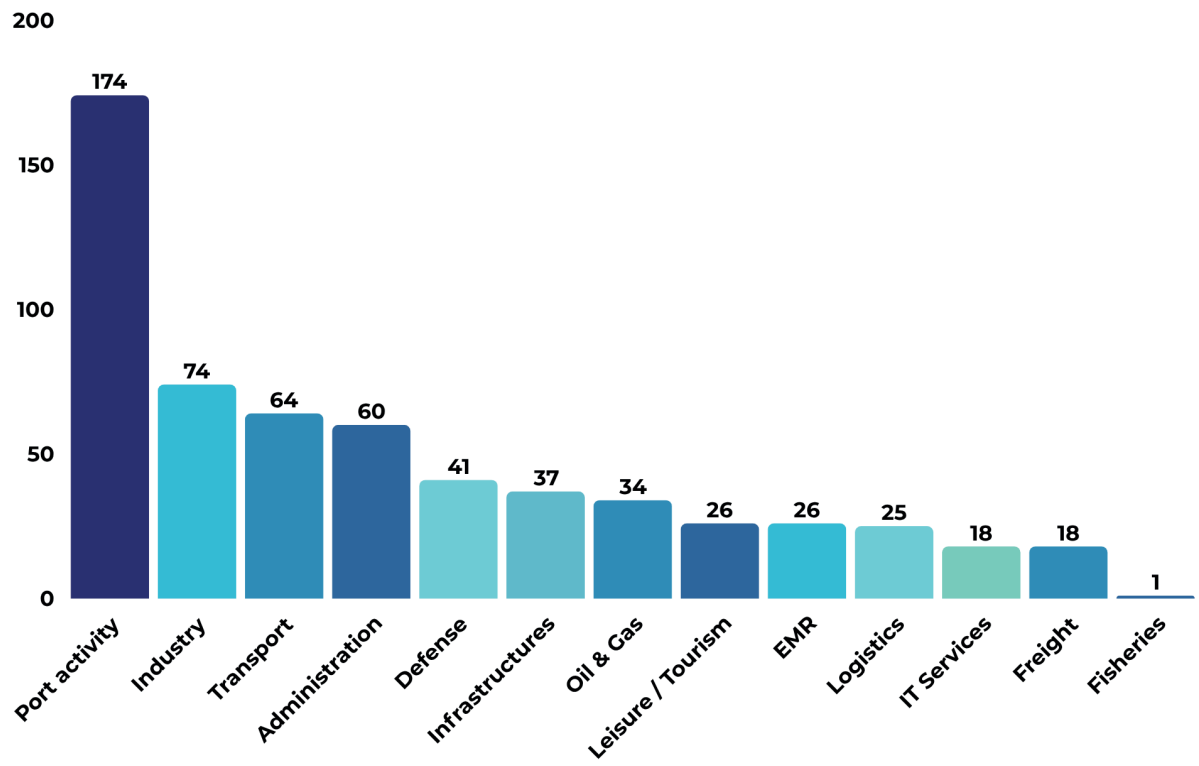
THREAT ACTOR TYPE	2024	2025
Hacktivism	370	500
Cybercrime	223	418
Undisclosed	8	16
State-sponsored	2	2

NIS2 CLASSIFICATION OF VICTIMS

THREAT ACTOR TYPE	2024	2025
NC – Non-classified	50.5% (305)	61.4% (574)
EE/IE – Essential/Important entity	49.5% (278)	38.7% (334)

INCIDENTS BY MARITIME SECTOR - 2024

Sector-level granularity was only available for 2024 data.



TOP THREAT ACTORS (EXCLUDING UNDISCLOSED)

RANK	2024	INCIDENTS	2025	INCIDENTS
1	NONAME057(16)	209	NONAME057(16)	177
2	CYBER_ARMY_RU	34	MR-HAMZA	96
3	LOCKBIT 3.0	22	QILIN	45
4	RANSOMHUB	18	AKIRA	40
5	CYBER_DRAGON	15	CLOP	37
6	RTFANNC	13	DARK STORM TEAM	27
7	AKIRA	12	HEZIRASH	24
8	PLAY	12	PLAY	23

KEY TREND

Incident volume surged +55% from 2024 to 2025. While DDoS by hacktivists remains the dominant attack type, cybercrime operations (ransomware and data leaks) are gaining significant ground — data leaks alone jumped +266% year-over-year. The US, Israel, Spain and Italy are consistently the most targeted nations.

TOP TARGETED COUNTRIES (TOP 10)

RANK	2024	INCIDENTS	2025	INCIDENTS
1	United States	108	United States	185
2	Spain	62	Israel	96
3	Italy	38	Italy	65
4	Ukraine	35	France	45
5	Germany	27	Spain	43
6	Israel	25	United Kingdom	33
7	United Kingdom	25	Canada	26
8	Sweden	24	Thailand	24
9	Japan	24	Poland	24
10	France	20	India	24

2.

THE GEOPOLITICAL BACKDROP



Contribution from FMES — Fondation pour la Maîtrise des Enjeux Stratégiques, a French think tank dedicated to strategic research, reflection and training at the crossroads of geopolitics, defence and technology.

THE ESCALATING MARITIME GEOPOLITICAL TENSIONS

At sea, geopolitical rivalries tend to harden more rapidly than elsewhere. Maritime areas have increasingly become places where economic, security and power interests converge and confront each other. International trade and globalization have made maritime transport central to the world economy: it now carries more than 80% of global trade by volume, leaving supply chains heavily dependent on sea routes. The ocean also holds strategic submarine cables and coveted fishery and mineral resources, adding to these tensions.

The intensification of great-power rivalries (United States, China, Russia…) and regional conflicts has led to a multiplication of maritime areas of conflict and tension: from the South China Sea, to the Persian Gulf and the Red Sea, up to the Baltic and the Arctic seas, both state and non-state actors use a range of means to pursue and defend their interests. Far from populated areas, confrontations at sea tend to take unconstrained and sometimes intense forms, as seen with the Russia-Ukraine war in the Black Sea, the Houthis in the Red Sea, or Chinese fishing fleets in the South China Sea. Private actors such as shipowners, port operators and offshore energy companies become caught up in these tensions: vessels carrying hazardous materials, valuable goods or fuel become strategic and vulnerable targets.

CYBER OPERATIONS AS A TOOL OF HYBRID WARFARE

Contemporary conflicts are shaped by hybrid warfare, a mix of military and non-conventional methods that sits below the threshold of armed conflict and blurs the lines of the traditional battlefield. Cyberspace, invisible and borderless, is a natural arena for it: its complexity and lack of norms make it a feared battlefield.

When no actor claims responsibility, it is hard to tell whether a cyber-system failure comes from internal malfunction or external interference. Hacking is a low-cost endeavour compared with the heavy measures needed to defend against it: small groups, such as hacktivists, can cause widespread digital disruption against far more powerful competitors.
Maritime organisations, vessels, navigation systems and harbour infrastructures are targeted by cyberattacks to disrupt operations by altering data, delaying cargo flows, or even causing collisions by making vessels undetectable or taking remote control of them. In 2017, a series of collisions involving US military vessels in Asia, some fatal, raised suspicions of a potential cyberattack. Offensive operations targeting GPS denial are increasingly reported across maritime regions, notably the Strait of Hormuz and the Gulf, where 20% of global oil traffic transits and GPS interference causes unreliable vessel positioning and AIS anomalies.
In 2025, the French National Cybersecurity Agency (ANSSI) estimated that cyberattacks on both public and private sectors increased by 15%. CyberOwl, a cybersecurity company, estimates that a typical fleet of 30 vessels experiences approximately 7 cyberattacks per month, while only 32% of shipowners include cybersecurity in their teams. But preventing cyberattacks requires new protective software and defensive tools, at significant cost. Building cyber resilience now calls for closer cooperation between public and private sectors, as geopolitical shocks and hybrid threats expose how interdependent the digital infrastructure really is.



3.

TWO THREATS, ONE NAME: REFRAMING 2025'S MARITIME INCIDENTS



Contribution from XRATOR, cybersecurity threat intelligence and analysis

Each year, global cyber reports converge on the same themes: more capable ransomware, exploited remote-access devices, and rising concern about AI in the hands of cybercriminals. Looking at 2025's maritime incidents, that picture is incomplete. Open sources point to roughly fifty notable maritime events. They form two families that share little in common.

The first is conventional, financially-motivated ransomware: about sixteen events against the IT of maritime intermediaries (agencies, ship managers, shipyards, terminals). The actors were not maritime specialists but the same groups active in every sector. Qilin appears in five maritime cases, alongside Akira, Clop and others. This matches the pattern in ENISA and Verizon's 2025 data: data theft and double extortion, with intermediaries prized as concentration nodes of the ecosystem. Here, shipping is a target like any other, exposed mainly through its suppliers.

The second family has no clear equivalent ashore, and IT-focused reports rarely count it: around twenty events against positioning and identification systems (GNSS and AIS). Part is electronic-warfare interference reaching civilian traffic in contested areas (the Baltic, the Strait of Hormuz, the Red Sea, the Caribbean). Part is deliberate spoofing by vessels to evade sanctions, documented by maritime-tracking analysts. By incident count, this navigation layer rivals ransomware, yet it is largely absent from mainstream cyber reporting.

The distinction matters because the two families need different risk owners and different controls. One is a criminal market seeking payment; the other is geopolitics and fraud conducted through the radio-navigation layer.

On artificial intelligence, the 2025 evidence is measured rather than alarming. None of the catalogued maritime incidents showed an AI-driven attack. Adversarial use of AI reported across sectors by Google's and Anthropic's threat teams accelerates existing techniques (phishing, fraud, scripting) but has produced no autonomous breach and no marked spike, only the continuation of existing trends. The year's most consequential maritime case was physical: French authorities found a remote-access device installed aboard a passenger ferry by a crew member acting for a foreign state. Where AI is maturing fastest is defence: security testing before production, and alert triage.

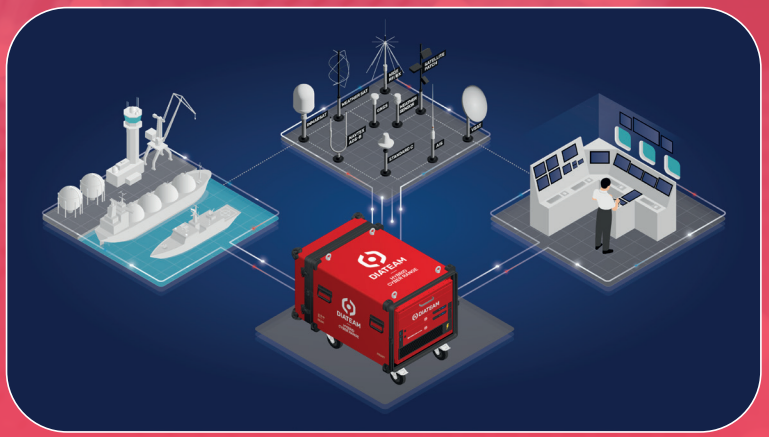
What is mainstream elsewhere and still emerging here is the commodity intrusion chain: stolen credentials, brokered access, exploited edge devices. Early signs: a port agency serving hundreds of ports breached through its supply chain, and an IT-provider compromise that propagated to a fleet. It signals where maritime is heading.

Security, safety and compliance officers should extend cyber and breach-notification requirements across the supplier chain (consistent with NIS2) and keep operational technology beyond navigation (cargo, terminal and crane systems) in scope. Fleet and port operations managers should treat navigation without reliable GNSS as a standing operational risk, with degraded-mode procedures and crew drills; even when your own vessel is not jammed, another crossing your route may be. Decision-makers should fund the two families separately: ransomware exposure mirrors every other industry, while positioning resilience is specific to maritime. The solutions exist; 2025 simply showed which ones the sector still treats as someone else's problem.

4.

PORT SECTOR SPOTLIGHT: REHEARSING THE ATTACKER'S PLAYBOOK

Contribution from DIATEAM,
a CY4GATE Compagny
Amélie GAUTIER, Business Engineer



DIATEAM Maritime Hybrid Cyber Range

Founded in 2002, DIATEAM is a global leader in the Hybrid Cyber Range and digital infrastructure prototyping market, with a particularly strong focus on the maritime sector. Its missions are: cybersecurity training for professionals in the maritime and port sectors using realistic simulations covering both IT and OT environments; state-of-the-art simulation of state-sponsored adversaries or cybercriminals in a maritime context; and the provision of Hybrid Cyber Ranges for digital-twin and prototyping platform purposes.

CYBER ATTACKS ON EUROPEAN PORTS IN 2025

In February 2025, an intrusion disabled the Port Community System of a North Sea port – logging ship movements, crew manifests, and cargo flows. The TTPs observed across maritime ransomware operations affecting the wider port ecosystem in 2025 followed a recurring pattern: exploitation of cybersecurity edge appliances, credential reuse from infostealer logs sold by initial access brokers, spear-phishing of finance and logistics teams, and pivots through compromised MSPs.

Open-source monitoring recorded 149 port-sector cyber incidents in 2025, overwhelmingly DDoS (132 cases, 88.6%), driven by pro-Russian collective NoName057(16) and concentrated on Italy (47 cases, nearly a third of the total), Poland, Finland, Spain, Belgium and Lithuania – a continuation of the post-2022 hybrid posture against NATO members. Direct ransomware against port authorities was rare (8 cases, only one in the EU); the broader maritime ecosystem upstream of port operations – shipping lines, agencies, equipment makers, software suppliers – absorbed the bulk of ransomware activity, with 18 ransomware attacks on logistics. Hacktivist impact stays bounded while DDoS stops at marketing sites; the Italian national PCS has been hit during ten campaigns since 2023, four in 2025 alone, alongside waves on Adriatic and Tyrrhenian port authorities.

External dependencies define the real attack surface. A US software vendor serving port operators was compromised in September, exposing clients downstream – the legitimate-looking access of MSPs, cloud providers, unmaintained third-party libraries, and insiders, with fewer detection signals. On the Baltic coast, sustained electronic warfare left GPS positioning unavailable around 17% of the time during 2025 peak months; falsified AIS and degraded positioning erode VTS and pilot situational awareness when it matters most.



DIATEAM Hybrid Cyber Range crisis-management exercise

Inside container terminals, IT/OT/IoT/5G convergence creates lateral paths that conventional segmentation rarely contains; the RF perimeter (WiFi, private 5G, IoT, AIS, GNSS) and physical vectors (USB, badge cloning, field devices) extend the surface most ports do not map. AI lowers the production cost of BEC and accelerates vulnerability discovery against exposed port systems.

Closing the gap requires training the way attackers operate: adversarial campaigns sustained over time, run across the extended perimeter – terminal operators, IT providers, logistics subcontractors – stress-testing detection, decision-making, and resilience under realistic pressure. DIATEAM has built this capability for the maritime sector over more than a decade, combining red team operations with a Hybrid Cyber Range that mirrors live ship and port systems (ECDIS, AIS, GPS, SATCOM, OT). "We don't sell cyber tools; we sharpen how your teams use the ones you already have. If you operate a port and want to see your attack surface through a determined adversary's eyes, talk to us."

5.

OT SYSTEMS IN THE EYE OF THE STORM

Contribution from Orange Cyberdefense, Ludovic JAMART, Consulting and Audit Director – Western France, Orange Cyberdefense France

The year 2025 demonstrated that the maritime and port sector can no longer ignore the cyber threat. Studies show a doubling of cyberattacks targeting the sector in 2025, focusing in particular on OT (Operational Technology) equipment — hardware and software that directly controls the critical functions of vessels and port infrastructures, increasingly exposed due to accelerated IT/OT convergence and extended shore-to-sea connectivity.

AMONG THE MOST SIGNIFICANT INCIDENTS

The cyberattack against Fanava, the Iranian VSAT service provider, took place in March and August 2025. Attributed to the Iranian hacktivist group Lab Dookhtegan, it neutralized shore communications for more than 150 vessels of the National Iranian Tanker Company and Islamic Republic of Iran Shipping Lines fleets. The attack followed a textbook supply-chain pattern: intrusion into Fanava's land-based hub to reach the connected fleet, administrator access on the VSAT terminals, and disabling of the iDirect Falcon satellite service — breaking ship-to-shore links and paralyzing AIS transponders. And finally a wiping technique deleted terminal configuration data and logs, grounding the vessels for weeks pending manual reinstallation.

The grounding of the MSC Antonia in May 2025 on the Eliza Shoals coral reefs in the Red Sea illustrates the collateral damage suffered by maritime transport actors near armed-conflict zones. While heading towards Jeddah, the MSC Antonia entered a "spoofing bubble": its GNSS receivers picked up false signals that disoriented the navigation instruments (AIS, ECDIS), displaying an erroneous position — with jumps of more than 6,000 km — and making trajectory recalculation impossible. At night, without reliable visual cues, the crew could not avoid grounding. The incident, which caused no casualties or pollution, highlights the danger of blind trust in digital navigation tools and the lack of cyber resilience in onboard systems.

The campaigns carried out by the Russian cyberattack group APT28 (also known as Fancy Bear) targeted the logistical and port infrastructures of several NATO countries supporting Ukraine, particularly Hamburg and Rotterdam. Based on current knowledge, these campaigns primarily allowed reconnaissance and pre-positioning, relying on brute-force attacks, credential theft, spear-phishing (rigged transport or customs documents) targeting key port-ecosystem users, exploitation of known vulnerabilities, and abuse of cloud services or legitimate software to maintain undetected persistence. The objectives are to collect information on cargoes, dates and routes of logistical and military aid transiting through ports, and to access IP camera systems or IT/OT gateways to potentially control port-terminal management systems. To date, no act of sabotage has been observed.

A REGULATORY RESPONSE TAKES SHAPE

International maritime authorities are responding. On 4 April 2025, the IMO published Revision 3 of circular MSC-FAL.1/Circ.3 on maritime cyber risk management guidelines, strengthening the framework by:

- Adding the "Govern" function to the risk-management process, requiring a person responsible for cybersecurity and resources, with the authority and support necessary for their duties.
- Drawing attention to OT systems and third-party risk.

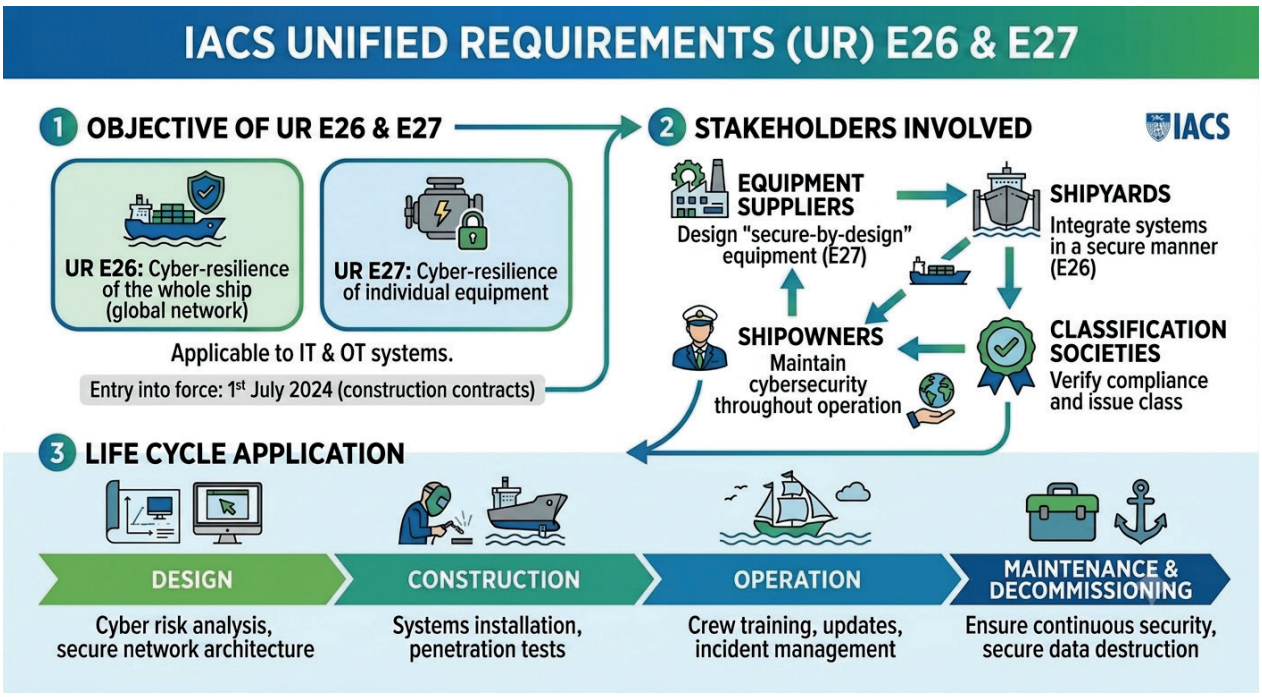
Despite these advances, the IMO circular remains non-binding under international law.

The most notable progress regarding a maritime cybersecurity framework comes from the IACS (International Association of Classification

Societies), which introduced Unified Requirements (UR) E26 and E27 on the cyber resilience of onboard systems and equipment. These became mandatory for all new vessels contracted after 1 July 2024, covering all computerised IT and OT systems across the vessel's lifecycle — design, construction and operation — for all classified vessels over 500 GT on international voyages. Majority of IACS member classification societies have aligned their class notation with UR E26 and E27.

A first step toward *Maritim security by design*

Orange Cyberdefense is the cybersecurity subsidiary of the Orange Group, with more than 3,300 experts across 12 countries and 36 detection centres worldwide, building a safer digital society by supporting organisations across the entire cyber threat lifecycle: anticipation, detection, incident response, and securing critical IT and OT systems.



6.

THE SEA-SHORE LINK: A NEW FRONTIER



Contribution from Marlink, maritime connectivity and cyber threat intelligence

ATTACK SURFACE AND KEY VECTORS

In 2025, the sea-shore link — satcom terminals, remote-access platforms, fleet-IT systems, AIS/GNSS inputs, port-call channels and shore IT/OT — became the most strategically vulnerable area of the maritime operating environment. The major threat has shifted from compromise of individual vessels to supply-chain attacks at the provider and OEM level that can affect entire fleets. Reported maritime cyber incidents increased by about 100% year-on-year (CYTUR/SAFETY4SEA data), and impacts shifted from mainly theft-related to more denial, destruction and physical-safety consequences.

KEY JUDGEMENTS

- Ransomware and double extortion against shore networks, providers and remote-access paths is the most frequent category of sea-shore incident in 2025.
- Supply-chain compromise of satcom/software providers is the highest-consequence vector — a single foothold enables fleet-wide effects.
- GNSS/AIS interference in contested waters (Strait of Hormuz, Red Sea, Black Sea) is now a persistent operational cyber-physical risk.
- State-linked actors continue to be the highest-consequence threat through espionage and pre-positioning.
- Regulatory momentum (USCG MTS Rule, IMO, IACS) will raise the baseline but will not close the exposure gaps within the 2025 timeframe, given phased timelines and legacy-system constraints.

THREAT ACTORS

Four categories of actors are active against the sea-shore link, differentiated by intent and consequences:

State and state-linked actors: the highest-consequence threat. Mustang Panda (China) targeted cargo-shipping firms in Norway, Greece and the Netherlands; APT41 struck shipping and logistics across the UK, Italy, Spain, Turkey, Taiwan and Thailand; Iran-linked Crimson Sandstorm targeted Mediterranean maritime operators; Russia-linked Turla/Tomiris and RedCurl conducted industrial espionage against transportation and logistics targets. Access established now enables later coercion or disruption.

Organised criminal groups: the most common disruptors. Double-extortion ransomware combines encryption with data-theft threats, targeting shore-side providers and exposed remote-access appliances. Financial motivation, but the operational consequences are indistinguishable from deliberate disruption.

Hacktivists: typically limited to DDoS and leaks, but the Lab Dookhtegan / Fanava operation (see also OT Systems in this report) demonstrated fleet-level reach via a satcom provider compromise, blurring the line with state-relevant destructive operations.

Insiders and contractors: retain a structural advantage through authorised access. In a heavily outsourced ecosystem, the insider perimeter extends to managed-service and satcom providers, as shown by the Ferry Fantastic case.



Maritime SOC monitoring global fleet connectivity — Source: Marlink

STRUCTURAL VULNERABILITIES

Highly connected safety-critical systems — including those connected to shore vendors, satellite links, or shared credentials — are the most exposed. Two structural vulnerabilities stand out:

Satcom terminal as a single point of failure: many of these units were designed for connectivity, not resilience. Compromise of a terminal gives the adversary control of all vessel communications, and a pivot into onboard IT and, in poorly segmented environments, OT.

Provider concentration: satcom operators, managed-IT integrators, software vendors and update servers concentrate risk — one compromise can propagate to many vessels or terminals at once.

Condensed from Marlink CTI — "Overview of Threats and Attacks on the Sea-Shore Link". Contact: cti@marlink.com

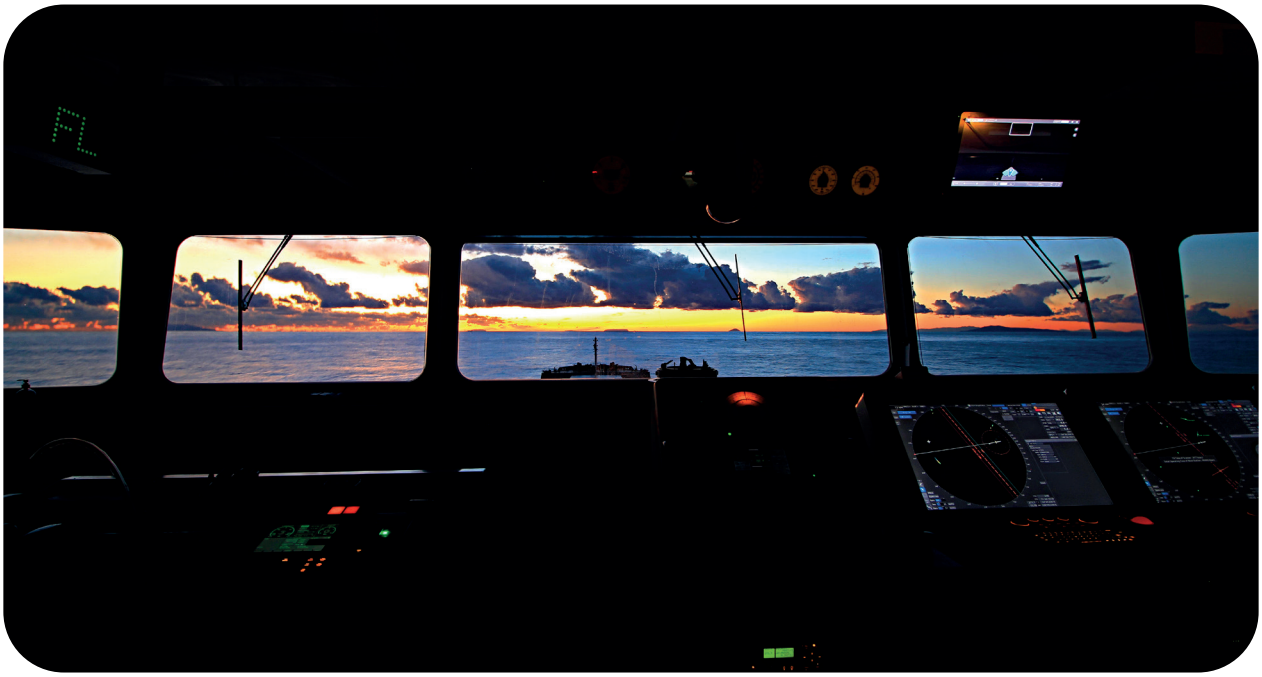
PRIMARY ATTACK VECTORS IN 2025

Phishing and credential theft: 43% of USCG-reported MTS cyber incidents in 2025 used phishing for initial access (up from 25% in 2024); compromised accounts weaponised for follow-on campaigns.

Supply-chain / third-party: the DNV ShipManager, Furuno, and Lab Dookhtegan / Fanava cases demonstrate two tiers — SaaS platform compromise and OEM compromise — both with fleet-wide reach. Remote-access appliances: exposed VPNs, RDP and management interfaces (including Citrix NetScaler CVEs) used as initial-access vectors.

Removable media and insiders: USB-borne infections documented across Turla/Tomiris campaigns and the Ferry Fantastic intrusion.

PNT manipulation: GNSS jamming and spoofing endemic in Hormuz, the Red Sea and the Black Sea; cascading effects on ECDIS, AIS, gyro, collision-avoidance and port-arrival planning.



Bridge navigation systems at dusk — Source: Marlink

7.

SPOTLIGHT: AIS SPOOFING — FROM DISAPPEARANCE TO DECEPTION

Contribution from Semsoft (LESTR), data fusion and AI for maritime trade-risk detection

Semsoft, a French technology company specialising in data fusion and artificial intelligence, has developed LESTR (the Breton word for "vessel," and an acronym for "Limit your Exposure to Sanctions and other Trade Risks"), a tool that detects illicit activity hidden within legitimate maritime trade and cargo operations.



For decades, illicit maritime operators pursued a simple objective: avoid detection. Initially, deception was largely physical — changing a vessel's name, appearance, or flag was often sufficient.

The widespread adoption of the Automatic Identification System (AIS), combined with satellite monitoring, changed the way vessels could be tracked. Maritime activity became transparent, giving security actors unprecedented visibility over vessel movements.

As transparency increased, operators adapted: rather than disguise themselves physically, many vessels simply went dark. These voluntary AIS gaps quickly became one of the clearest signs of sanctions evasion, illicit ship-to-ship (STS) transfers and embargo circumvention. But the strategy became a victim of its own success: today an unexplained AIS gap is often enough on its own to trigger scrutiny. In many cases, disappearing has become more suspicious than staying visible.

Maritime evasion has grown markedly more sophisticated. Instead of disappearing, vessels now increasingly stay visible while broadcasting false information — a practice known as AIS spoofing, in which data is deliberately altered to conceal a vessel's true identity or location and mask illicit activities.

Early spoofing attempts were often crude. Analysts occasionally observed vessels operating in impossible locations or broadcasting obviously false identifiers; such anomalies were relatively easy to detect.

Identity-related spoofing has grown far more sophisticated. Basic schemes rely on transmitting false vessel names, MMSI numbers, call signs or IMO numbers — a tactic long seen in North Korean sanctions evasion, as with the tanker An San 1. More advanced operations, sometimes called "vessel identity laundering," appropriate the identity of a legitimate vessel to give cover to one engaged in illicit activity: the goal is no longer to hide, but to become someone else.

Location is evolving the same way. Rather than generating impossible trajectories, operators now replay legitimate historical AIS sequences, so an analyst relying on AIS alone sees a plausible route while the vessel's real activity happens elsewhere. This was seen with the LNG tanker IMO 9307205, which broadcast a false location in Malaysian waters to mask its presence alongside a sanctioned vessel during a clandestine ship-to-ship transfer of Russian gas — behaviour that contributed to its blacklisting by UK authorities.

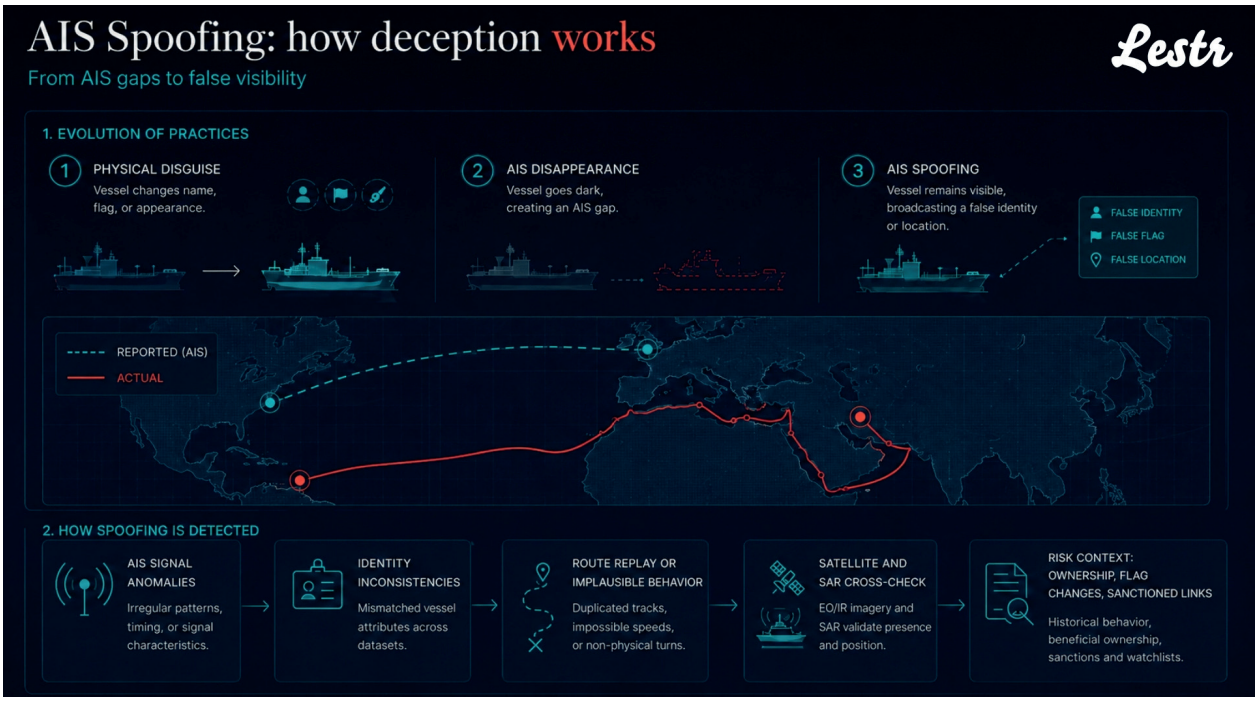
This shift reflects current geopolitical reality. The tightening of sanctions against Russia, Iran, and North Korea has created strong incentives to conceal illicit energy flows, accelerating the development of increasingly sophisticated maritime deception schemes.

Detecting such practices requires combining multiple sources of evidence. Modern analysis relies on signal-first approaches to analyse AIS messages for inconsistencies and anomalies. Simultaneously, image-first approaches allow for the comparison of AIS-reported positions with satellite imagery and SAR observations. Increasingly, radio-frequency intelligence provides an independent means of confirming vessel presence even when AIS data has been manipulated.

However, spoofing should not be viewed as an isolated indicator. Vessels engaged in sophisticated deception often share other high-risk characteristics, including the lack of P&I insurance, a history of deficiencies in Port State Control inspections, and frequent changes of name or flag.

Ultimately, the challenge extends beyond AIS itself. What is at stake is the reliability of the information used to monitor and secure maritime activities. Today, the vessels that concern us most are often not the ones that go dark, but the ones that remain visible while broadcasting a false reality.

Evolution of evasion practices — physical disguise, AIS disappearance and AIS spoofing — and how analysts detect it: signal anomalies, identity inconsistencies, route-replay, satellite/SAR cross-checks and risk-context review. Source: LESTR / Semsoft



8.

MAJOR VULNERABILITIES EXPLOITED IN 2025, AND TRENDS

Contribution from GLIMPS
AI-powered deep file analysis and malware characterisation

In 2025, France is facing a sharp increase in cybersecurity incidents and data breaches. More than 6,000 personal data breach notifications were filed with the CNIL, a historically high level affecting all sectors: public administration, healthcare, education, industry, financial services, and major digital platforms. Financial and reputational stakes continue to grow.

This surge in breaches is a reminder of the importance of staying vigilant against phishing and social engineering. Campaigns are becoming increasingly convincing, notably through AI, which generates emails, fake websites, and messages at scale, highly believable and in all European languages.

At the same time, a slight decline in ransomware attacks has been observed, though it remains relative: criminal groups are adapting their methods rather than disappearing. Among the most active: Qilin, Akira, ClOp, Play, and LockBit. Operators are becoming more aggressive. Encryption is no longer systematic, while mass data theft, threats of exposure, and pressure on partners and clients have become the preferred leverage. Combined with AI, this foreshadows even more sophisticated campaigns in the future.

Legitimate administration tools have always been present in attack chains, but their use has become nearly systematic. Attackers favor well-known, trusted tools to blend into normal system activity or exploit vulnerable versions, making malicious activity far harder to detect and block.



VULNERABILITIES: SEVERITY AND REPORTING

Two complementary perspectives emerge.

By severity, CERT-FR issued only three top-level alerts over the year, all targeting widely deployed infrastructure: Citrix NetScaler (CVE-2025-7775, remote code execution), Cisco ASA/FTD VPN (CVE-2025-20333/20362), and React Server Components (CVE-2025-55182, unauthenticated RCE); Fortinet FortiWeb (CVE-2025-64446) was flagged as actively exploited.

By volume of reports (across advisories and press coverage, an indicator of real-world impact), the ranking shifts: React RSC (CVE-2025-55182) tops the list, ahead of the Oracle E-Business Suite zero-day exploited by Cl0p (CVE-2025-61882), Fortra GoAnywhere MFT (CVE-2025-10035, CVSS 10.0), and the Microsoft SharePoint "ToolShell" chain (CVE-2025-53770/53771).

The common thread: exposed edge devices, file transfer and collaboration servers, exploited as zero-days within days of disclosure. The defensive priority is clear: rapid patching of perimeter systems and monitoring of remote access.

THE ROLE OF AI

In 2025, AI has moved from early experimentation to industrialized tooling across the entire attack chain:

Phishing automation: yes, and widespread. Mass generation of lures, fake sites, and highly convincing multilingual messages.

Vulnerability research: emerging. AI assists with code review and triage to surface flaws faster, though human expertise remains decisive.

Exploit script generation: emerging. AI helps draft and adapt proof-of-concept code and exploits, lowering the barrier to entry.

OUTLOOK

The 2025 picture is one of convergence: faster exploitation of perimeter vulnerabilities, stealthier intrusions via trusted tools, and an offensive arsenal augmented by AI. However, that same technology strengthens defense, accelerating detection, triage, and response for organizations that adopt it early.



Top 10 vulnerabilities by volume of reports, 2025

9.

WHEN THE TIDE TURNS: AI-DRIVEN CYBERATTACKS AND WHAT THE MARITIME SECTOR MUST WATCH FOR

Contribution from BZHunt, offensive cybersecurity, penetration testing and red-teaming

BZHunt is a French offensive cybersecurity firm based in Brittany, specialising in penetration testing, red-teaming and security audits across maritime and port infrastructure. Its teams combine bug-bounty heritage with field expertise to help operators anticipate threats rather than react to them.

Every captain knows the real danger is rarely the wave you see coming — it's the swell beneath the surface, the current that shifts unnoticed until the hull drifts off course. The same now holds in cybersecurity: behind the headlines about ransomware shutdowns, a quieter shift is under way — AI entering the attacker's toolkit.

A CHANGE OF PACE, NOT YET A CHANGE OF NATURE

The temptation, fed by vendor marketing, is to imagine AI conjuring entirely new categories of attack. Reality is more sober: when Anthropic presented its Mythos model as able to discover kernel-level vulnerabilities autonomously, researchers at Rival Security found the flagship case, CVE-2026-4747 in FreeBSD, to be a near-identical replay of CVE-2007-3999, an overflow patched in MIT Kerberos two decades earlier and likely present in the model's training data. Mythos did not invent; it recognised, recombined and exploited at machine speed.

Daniel Stenberg, creator of cURL, reached a similar verdict after Mythos scanned his project: of five claimed vulnerabilities, only one low-severity flaw held up. His take in The Register was that the breakthrough narrative was "primarily marketing," and that current AI tools find "the usual and established kind of errors we already know about. It just finds new instances of them."

WHY PORTS ARE WHERE THE TIDE HITS HARDEST

For a port authority or terminal operator, that nuance doesn't lower the threat level — it raises it. The exposure is no longer theoretical: since 1980, 542 publicly disclosed cyber incidents have hit ports worldwide, with another 117 hitting the broader logistics chain. Ports are, by a wide margin, the most targeted node of the maritime ecosystem.

It's worth separating two very different attack surfaces here. Shipowners contend with AIS, ECDIS and onboard navigation; ports face a denser picture — interconnected systems (PCS, CCS, TOS), vessel traffic services consuming AIS feeds without emitting them, industrial controllers on cranes and gates, IoT sensors across the quays, and increasingly private 5G — and most operators have also moved large parts of their IT to public clouds, widening the attack surface.

These are exactly the environments where forgotten vulnerabilities sleep, and where an AI assistant in an attacker's hands becomes formidable — not a genius, but a tireless pattern matcher sifting code faster than any human red team, finding the corners where 2007-era bugs were quietly copied into 2026 systems. Any serious port operator should assume it is being scanned constantly, and that an attacker has likely already found footholds, waiting for the right moment.

As cybersecurity strategist Matthew Rosenquist has noted, attackers hold a structural advantage: they can adopt unvetted, risky AI tools immediately, bearing no responsibility for collateral damage — defenders cannot. A misfiring AI filter in a port operations centre is, in his words, "an insider attack conducted by incompetent security."

PRACTICAL TAKEAWAYS FOR MARITIME DECISION-MAKERS

Three priorities deserve attention before the next budget cycle.

First, full-scope mapping of the port attack surface. Port community systems, terminal operating systems, VTS, industrial controllers, IoT fleets, private 5G and the cloud tenants hosting critical workloads need inventorying as one continuous perimeter, not siloed projects. Many applications carry components from old open-source libraries, and cloud outsourcing has widened the perimeter faster than security teams have grown. Knowing what runs, where, and exposed to whom, is no longer optional.

Second, offensive testing that goes beyond compliance. Traditional audits and automated scans will not surface the chained, cross-domain weaknesses a real adversary will exploit — the kind that link a misconfigured cloud bucket, a forgotten IoT gateway and a TOS workflow into one business-stopping incident. Ports need specialists who can master this whole stack and think like an attacker, probing where it really hurts under pressure — creativity that current models still lack.

Third, governance of AI inside your own perimeter. As shipping lines deploy AI copilots for crew support, predictive maintenance, or customer service, each new model becomes an attack surface and a potential data-leak channel.

The sea has always rewarded those who read the weather early. AI-driven attacks are not a future scenario. As on a ship, they are the current we are already sailing through. The question is whether your bridge crew has the instruments, and the partners, to keep the course.



10.

AI BECOMES A STRATEGIC ACTOR IN THE INFORMATION CONFLICT

Contribution from ATOS,
analysis of AI-driven information manipulation and the cognitive-warfare dimension of hybrid threats

Deepfake content has been exploding since 2025. The volume of deepfake files increased from around 500,000 identified contents in 2023 to more than 8 million in 2025 according to EUvsDisinfo. Fraud attempts using synthetic content have increased by 3,000%.

Since 2025, European states now officially refer to an "information threat." France has incorporated this dimension into its new doctrine. This shift is fundamental: it is no longer simply about disinformation or fake news, but about a genuine field of strategic conflict aimed at influencing perceptions, behaviors, and decisions of individuals, companies, and democratic societies.

This evolution is based on a simple reality: in our digital societies, data feeds everything. Data feeds information. Information produces intelligence. Intelligence guides political, economic, military, or societal decisions — including those of ship captains.

Therefore, if data is false, biased, or manipulated, the entire decision-making chain can be contaminated.

Several recent examples demonstrate the power of these threats. In the Strait of Hormuz, since February 28, manipulation of GPS, GNSS, and AIS signals has aimed to create false information and misleading intelligence to provoke an incident. Nearly one million satellite navigation interference incidents were reportedly recorded, affecting around 1,100 vessels on the very first day of the Iran war crisis, according to the MICA Center. Ships could appear in false positions: on land, in airports, or in inconsistent areas. These disinformation actions can lead to insurance errors, misjudgment of risk, unjustified rerouting decisions, or, conversely, dangerous exposure.

Maritime data and information have become both a strategic resource and a weapon.

A DATA-DRIVEN COGNITIVE WARFARE

Contemporary conflicts aim as much to destroy infrastructure as to alter perceptions and human behavior, notably through the use of AI. A false financial signal can trigger stock market panic. A manipulated video can discredit a leader.

An algorithmic campaign can polarize a population. Data manipulation using only 250 documents can produce erroneous analyses in AI systems.

The phenomenon has accelerated sharply since 2025, with the rise of new manipulation techniques.

DIVERSIONS

Recently, the FBI warned in April 2026 about the rise in cargo theft. The modus operandi is typically informational and facilitated by AI. Attackers impersonate carriers or brokers, publish fake freight listings, redirect cargo, manipulate documents or logistics instructions, or clone executives. Estimated losses related to cargo theft in the United States and Canada reached nearly $725 million in 2025, representing a 60% increase compared to 2024. This is only the beginning.

The problem now goes beyond simple disinformation. Information and cognitive warfare aim to influence emotions, collective reflexes, trust, and behaviors, and even neural patterns.

AI is the fourth actor in conflict, alongside states, organizations, and individuals. It triggers a historical disruption.

It is becoming a new autonomous actor capable of producing, synthesizing, personalizing, and disseminating information at industrial speed, continuously, and able to target anyone based on their interests or anxieties.

Generative AI can now:

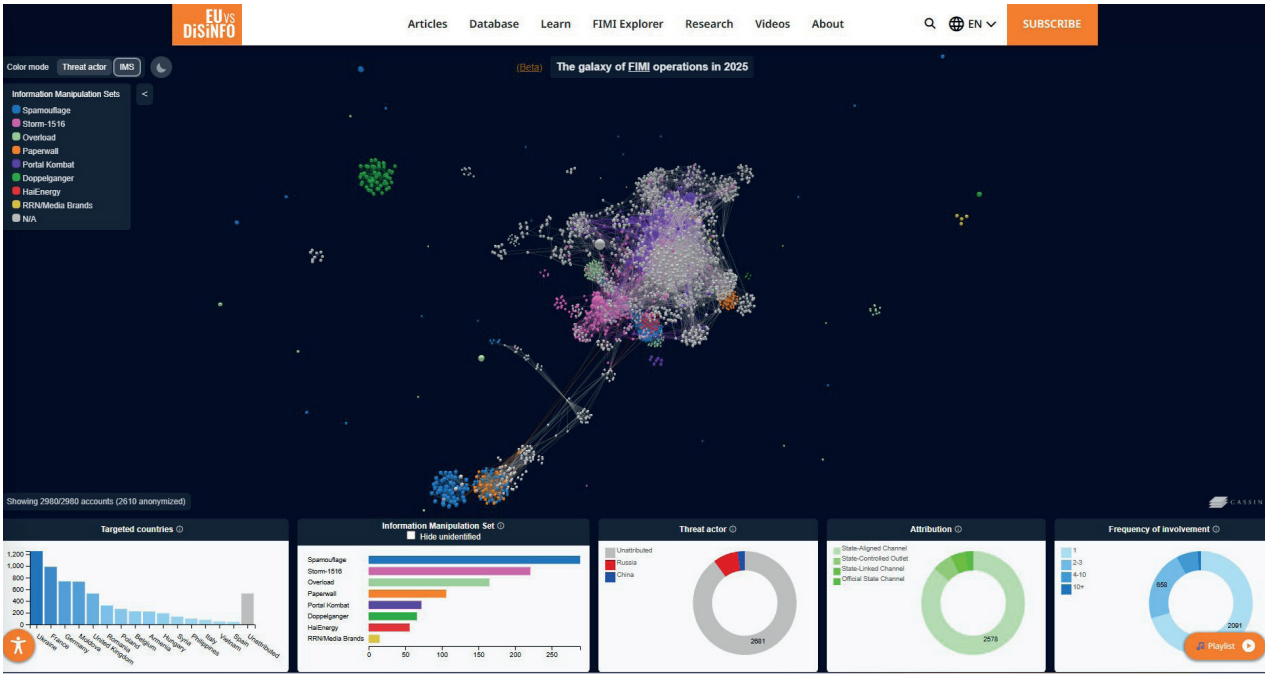
- produce thousands of credible articles, videos, or messages;
- clone human voices;
- create avatars of decision-makers;
- automate influence campaigns;
- personalize narratives according to psychological profiles or decision-makers' roles;
- cut off essential digital services for a single individual;
- fuel conversational agents capable of interacting massively with citizens or individually.

THE BATTLE AHEAD: PROTECTING SYSTEMS AND PERCEPTIONS

The new threat is informational. And AI is now becoming one of its main strategic accelerators — as well as a tool for defense.



Cette publication affirme montrer les conséquences d'un tir de missile iranien sur le porte-avions Abraham Lincoln. Une image générée par IA en réalité. - Publication X



11.

BUILDING OPERATIONAL RESILIENCE IN AN ERA OF HYBRID RISKS

Contribution from Alcyconie,
cyber crisis management company

FROM CYBER PROTECTION DO OPERATIONAL RESILIENCE

A cyber incident affecting a port community system, a terminal operating system or a critical maritime service can now disrupt cargo flows across multiple countries within hours. As maritime operations become increasingly interconnected, cyber risk has evolved from a purely technical concern into a strategic operational challenge for ports, shipping companies, maritime authorities and logistics stakeholders.

Drawing on experience gained through large-scale cyber crisis exercises conducted with maritime and port organisations across Europe, Alcyconie has observed a profound shift in the sector's approach to cyber risk. While organisations initially focused on strengthening technical protection and detection capabilities, **the most mature actors now recognise that resilience depends equally on their ability to maintain operations, coordinate stakeholders and make critical decisions under pressure.**

The maritime sector faces unique challenges. Unlike many industries, it operates within a highly interconnected ecosystem where disruption affecting a single organisation can rapidly propagate across shipping lines, terminal operators, logistics providers, pilots, customs authorities and public institutions. At the same time, maritime infrastructures sit at the heart of global trade and strategic competition. In several recent geopolitical crises, ports, shipping routes and logistics ecosystems have become direct or indirect targets of disruptive actions aimed at exerting economic, political or strategic pressure. As a result, cyber resilience is no longer solely an organisational matter. It increasingly relies on the collective ability of maritime communities to anticipate, withstand and respond effectively to crises that may combine cyberattacks, operational disruption, supply chain impacts and geopolitical dynamics.

STRENGHTENING GOVERNANCE AND CRISIS ORGANIZATION

The implementation of NIS2, combined with growing concerns about operational continuity, is accelerating the evolution of cyber crisis governance throughout the maritime sector.
Across the organisations supported by Alcyconie, several common priorities are emerging:

- Establishing clear alerting, escalation and decision-making processes extending beyond technical teams;
- Integrating critical suppliers, subcontractors and operational partners into crisis management frameworks;
- Strengthening business continuity and recovery plans for essential maritime services and logistics operations;
- Enhancing coordination between executive leadership, operational teams and cybersecurity specialists.

These developments reflect a broader understanding that cyber incidents can no longer be treated solely as IT events. In maritime environments, disruptions may affect vessel operations, cargo management, logistics chains, communications or public services, requiring coordinated responses across multiple functions and organisations.

As a consequence, cyber crisis exercises have become a central component of resilience programmes, enabling organisations to validate governance structures and identify potential weaknesses before a real incident occurs.

EXERCISING FOR THE CRISIS OF TOMORROW

While ransomware, denial-of-service attacks and system compromises remain major concerns, maritime organisations increasingly recognise that future crises are likely to combine cyber, operational, informational and geopolitical dimensions. The nature of exercises has therefore evolved significantly.

For organisations beginning their resilience journey, exercises primarily focus on validating crisis management frameworks, clarifying responsibilities and improving coordination between technical, operational and executive stakeholders.

For more mature organisations, objectives are broader. Exercises increasingly involve operational technology environments, business units, executive committees and external partners. The focus shifts from technical response towards strategic decision-making, continuity of operations and stakeholder coordination under uncertain conditions. This evolution reflects the changing threat landscape.

For a sector that sits at the frontline of global trade and geopolitical tensions, strategic foresight is no longer optional. Maritime organisations must continuously look beyond current threats and develop the ability to anticipate emerging forms of disruption. Whether driven by technological innovation, geopolitical instability, supply chain dependencies or hybrid influence operations, future crises are unlikely to resemble those of the past. Building resilience therefore requires not only preparedness, but also a culture of anticipation and continuous adaptation.

In this context, cyber crisis exercises are increasingly used as a tool for strategic foresight. Beyond validating existing procedures, they enable organisations to explore plausible future scenarios, challenge assumptions and prepare decision-makers for crises that have not yet occurred, but could significantly affect maritime operations and business continuity.

Growing geopolitical tensions, supply chain interdependencies, reliance on critical third parties and the emergence of hybrid threats are creating scenarios whose consequences extend well beyond information systems. Maritime organisations are increasingly exposed to situations where multiple disruptions occur simultaneously: compromise of a strategic supplier, prolonged unavailability of operational systems, disruption of logistics chains, disinformation campaigns targeting port activities, or coordinated actions designed to undermine trust and operational performance.

Over the past year, Alcyconie has notably developed advanced crisis simulations for major international maritime stakeholders, including scenarios combining cyberattacks, operational disruptions and influence operations. These exercises are designed not to predict the next crisis, but to expose organisations to plausible situations that challenge existing assumptions and test their ability to adapt under pressure.

LESSONS LEARNED FROM MARITIME CRISIS EXERCISES

Several recurring observations emerge from the exercises conducted with maritime and port organisations:

- Operational impacts are often underestimated compared to technical impacts;
- Dependencies on suppliers and external service providers frequently represent critical vulnerabilities;
- Executive-level decision-making plays a decisive role in limiting the consequences of an incident;
- Communication with customers, partners, authorities and the media rapidly becomes a strategic issue;
- Coordination across the maritime ecosystem is often more challenging than technical remediation itself.

These findings illustrate a broader transformation in cyber preparedness. Organisations are no longer seeking only to improve their ability to detect and respond to cyberattacks. They increasingly aim to strengthen their capacity to maintain operational control, preserve critical services and make informed decisions despite uncertainty and incomplete information.

LOOKING AHEAD

The maritime sector sits at the crossroads of global trade, strategic infrastructure and geopolitical competition. As cyber threats continue to evolve, resilience can no longer be measured solely by the strength of technical defences.

The organisations that will prove most resilient are those capable of maintaining operational continuity, coordinating effectively across complex ecosystems and making critical decisions under pressure.

In an environment where cyber, operational, informational and geopolitical risks increasingly converge, resilience has become a collective capability. For maritime stakeholders, preparing for this reality through realistic and ambitious crisis exercises is no longer an option—it is becoming a strategic necessity.



CONTRIBUTORS TO THIS EDITION

FRANCE CYBER MARITIME THANKS THE FOLLOWING ORGANISATIONS FOR THEIR CONTRIBUTIONS TO THIS REPORT.

Alcyconie — cyber crisis management company, PACS qualified by ANSSI.

ATOS — analysis of AI-driven information manipulation and the cognitive-warfare dimension of hybrid threats.

BZHunt — offensive cybersecurity, penetration testing and red-teaming, Brittany, France.

DIATEAM — Hybrid Cyber Range and maritime cybersecurity training.
• contact@diateam.net

FMES (Fondation pour la Maîtrise des Enjeux Stratégiques) — French strategic-research think tank.

GLIMPS — AI-powered deep file analysis and malware characterisation, built on sovereign Deep Learning technology.

Marlink — maritime connectivity and cyber threat intelligence.
• cti@marlink.com

Orange Cyberdefense — cybersecurity subsidiary of the Orange Group.

Semsoft (LESTR) — data fusion and AI for maritime trade-risk detection.
• business@lestr.app

XRATOR — cybersecurity threat intelligence and analysis.

FRANCE CYBER MARITIME

Le Grand Large
Quai de la douane, 2ème éperon
29200 BREST

02 57 52 09 87
contact@france-cyber-maritime.eu

TLP.CLEAR TLP:EX:NC

www.france-cyber-maritime.eu

SUPPORTED BY

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

Brest Métropole

MINISTÈRE CHARGÉ DE LA MER ET DE LA PÊCHE
Liberté
Égalité
Fraternité

Région Bretagne

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la mer