
# + PANORAMA DE LA MENACE CYBER MARITIME 2025

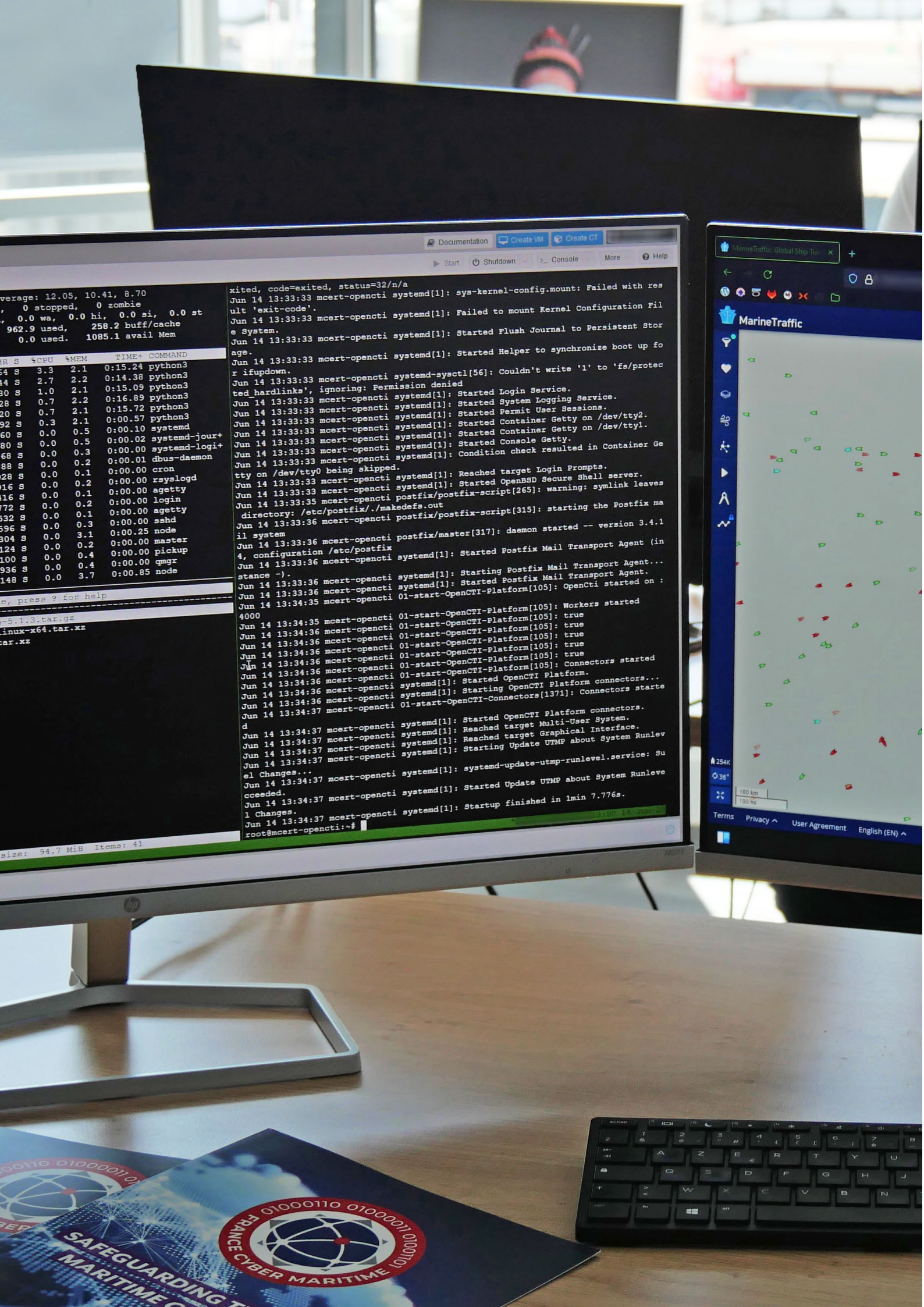
EN COLLABORATION AVEC

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

DANS LE CADRE DU PROJET EUROPÉEN

SAFEDIGIMAR
FOR A SAFER DIGITAL MARITIME EUROPE

Co-funded by
the European Union


Documentation
Create VM
Create CT
Start
Shutdown
Console
More
Help
verage: 12.05, 10.41, 8.70
0 stopped, 0 zombie
0.0 wa, 0.0 hi, 0.0 si, 0.0 st
962.9 used, 258.2 buff/cache
0.0 used. 1085.1 avail Mem
TIME+ COMMAND
0:15.24 python3
0:14.38 python3
0:15.09 python3
0:16.89 python3
0:15.72 python3
0:00.57 python3
0:00.10 systemd
0:00.02 systemd-jour+
0:00.00 systemd-logi+
0:00.01 dbus-daemon
0:00.00 cron
0:00.00 rsyslogd
0:00.00 agetty
0:00.00 login
0:00.00 agetty
0:00.00 sshd
0:00.25 node
0:00.00 master
0:00.00 pickup
0:00.00 qmgr
0:00.85 node
e, press ? for help
-5.1.3.tar.gz
inux-x64.tar.xz
ar.xz
size: 94.7 MiB Items: 41
xited, code=exited, status=32/n/a
Jun 14 13:33:33 mcert-opencti systemd[1]: sys-kernel-config.mount: Failed with res
ult 'exit-code'.
Jun 14 13:33:33 mcert-opencti systemd[1]: Failed to mount Kernel Configuration Fil
e System.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Flush Journal to Persistent Stor
age.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Helper to synchronize boot up fo
r ifupdown.
Jun 14 13:33:33 mcert-opencti systemd-sysctl[56]: Couldn't write '1' to 'fs/protec
ted_hardlinks', ignoring: Permission denied
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Login Service.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started System Logging Service.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Permit User Sessions.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Container Getty on /dev/tty2.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Container Getty on /dev/tty1.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Console Getty.
Jun 14 13:33:33 mcert-opencti systemd[1]: Condition check resulted in Container Ge
tty on /dev/tty0 being skipped.
Jun 14 13:33:33 mcert-opencti systemd[1]: Reached target Login Prompts.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started OpenBSD Secure Shell server.
Jun 14 13:33:35 mcert-opencti postfix/postfix-script[265]: warning: symlink leaves
directory: /etc/postfix/./makedefs.out
Jun 14 13:33:36 mcert-opencti postfix/postfix-script[315]: starting the Postfix ma
il system
Jun 14 13:33:36 mcert-opencti postfix/master[317]: daemon started -- version 3.4.1
4, configuration /etc/postfix
Jun 14 13:33:36 mcert-opencti systemd[1]: Started Postfix Mail Transport Agent (in
stance -).
Jun 14 13:33:36 mcert-opencti systemd[1]: Starting Postfix Mail Transport Agent...
Jun 14 13:33:36 mcert-opencti systemd[1]: Started Postfix Mail Transport Agent.
Jun 14 13:34:35 mcert-opencti 01-start-OpenCTI-Platform[105]: OpenCti started on :
4000
Jun 14 13:34:35 mcert-opencti 01-start-OpenCTI-Platform[105]: Workers started
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: Connectors started
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI Platform.
Jun 14 13:34:36 mcert-opencti systemd[1]: Started OpenCTI Platform connectors...
Jun 14 13:34:36 mcert-opencti systemd[1]: Starting OpenCTI Platform connectors...
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Connectors[1371]: Connectors starte
d
Jun 14 13:34:37 mcert-opencti systemd[1]: Started OpenCTI Platform connectors.
Jun 14 13:34:37 mcert-opencti systemd[1]: Reached target Multi-User System.
Jun 14 13:34:37 mcert-opencti systemd[1]: Reached target Graphical Interface.
Jun 14 13:34:37 mcert-opencti systemd[1]: Starting Update UTMP about System Runlev
el Changes...
Jun 14 13:34:37 mcert-opencti systemd[1]: systemd-update-utmp-runlevel.service: Su
cceeded.
Jun 14 13:34:37 mcert-opencti systemd[1]: Started Update UTMP about System Runleve
l Changes.
Jun 14 13:34:37 mcert-opencti systemd[1]: Startup finished in 1min 7.776s.
root@mcert-opencti:~#
MarineTraffic
Terms
Privacy
User Agreement
English (EN)
01000110 01000011
FRANCE CYBER MARITIME
SAFEGUARDING
MARITIME

# SOMMAIRE

# AVANT-PROPOS

## DU DIRECTEUR DE FRANCE CYBER MARITIME

Le secteur maritime, portuaire et fluvial occupe une place essentielle dans nos économies et nos équilibres stratégiques. Il soutient les échanges, les chaînes logistiques et l'activité industrielle.

L'année 2025 confirme que la menace visant notre écosystème n'est plus périphérique ni théorique. Elle s'intensifie alors que tensions géopolitiques, criminalité organisée, hacktivisme et numérisation des opérations se renforcent mutuellement. Le M-CERT a recensé 936 incidents affectant le secteur maritime au niveau mondial en 2025, contre 604 en 2024, soit une progression de 55 %. Derrière ces chiffres : indisponibilités de services, fuites de données, extorsions, perturbations de la navigation et vulnérabilités des sous-traitants.

Ce panorama met en évidence une menace à plusieurs visages. Les attaques par déni de service, souvent portées par des collectifs hacktivistes, restent nombreuses. Mais la progression des logiques cybercriminelles, notamment les fuites de données et la double extorsion, appelle une vigilance renforcée. Systèmes de navigation, liaisons mer-terre, infrastructures portuaires, environnements industriels et fournisseurs numériques ou satellitaires deviennent des points de concentration du risque.

La spécificité maritime tient à l'imbrication entre systèmes d'information et opérations physiques, sûreté et sécurité. Une attaque cyber peut affecter la capacité à charger ou décharger, à guider et localiser autant que communiquer ou planifier. La cybersécurité maritime impose donc une compréhension fine des métiers, contraintes d'exploitation et dépendances propres à la mer et aux ports.

La réponse doit rester pragmatique. L'intelligence artificielle et l'automatisation offensive renforcent certaines capacités adverses, mais les fondamentaux demeurent : connaître son patrimoine numérique, cartographier ses dépendances, sécuriser les accès, corriger les vulnérabilités, préparer les modes dégradés, entraîner les équipes et organiser la réponse à incident.

Avec ce panorama, France Cyber Maritime, par ses adhérents et le M-CERT, souhaite contribuer à une lecture commune de la menace, sans entretenir l'inquiétude. Il s'agit de fournir aux acteurs du monde maritime et cyber des éléments utiles pour agir. La résilience du secteur dépendra de notre capacité collective à coopérer, partager les signaux faibles et tirer les enseignements des incidents.

Je remercie les contributeurs de cette édition. Leurs analyses témoignent de la maturité d'une communauté maritime cyber engagée. Plus que jamais, la cybersécurité est une condition de confiance et de continuité du secteur.

**Christian CÉVAËR**

# À PROPOS DE CE RAPPORT


## À PROPOS DE FRANCE CYBER MARITIME ET DU M-CERT

France Cyber Maritime est une association à but non lucratif (loi de 1901) dont la mission est de renforcer la cybersécurité du secteur maritime et portuaire français. Elle rassemble des organismes publics, des opérateurs maritimes et portuaires, ainsi que des prestataires de solutions de cybersécurité qualifiés.

France Cyber Maritime a pour objectifs de développer un réseau d'expertise en cybersécurité maritime en encourageant la création de services adaptés et d'accroître la résilience des acteurs maritimes et portuaires face aux cybermenaces en opérant le M-CERT (Maritime Computer Emergency Response Team), qui fournit informations et assistance au secteur.

Depuis mars 2021, le M-CERT surveille et analyse les menaces pesant sur le monde maritime et publie régulièrement des bulletins d'analyse à l'intention des membres, en plus d'assurer des services de prévention des risques, d'alerte et de coordination des interventions en cas d'incident, en collaboration avec les autorités publiques et d'autres organismes de cybersécurité.

## À PROPOS DE SAFEDIGIMAR

Fin 2025, la Commission européenne a officiellement signé une convention de subvention avec un consortium comprenant France Cyber Maritime, FEPORT et la Federazione del Mare, à la suite de leur candidature retenue dans le cadre de l'appel à propositions du projet SAFEDIGIMAR. Celui-ci vise à promouvoir la mise en oeuvre des mesures liées à la directive NIS2 et à développer des solutions sur mesure pour renforcer la cybersécurité de l'écosystème. Il assure le suivi des risques et des menaces pesant sur le secteur, diffuse les bonnes pratiques et apporte son aide aux victimes de cyberattaques issues de la communauté maritime.

## METHODOLOGIE

L'identification des incidents de cybersécurité touchant le secteur maritime présentés dans ce rapport a nécessité une veille quotidienne d'une série de sites web spécialisés et de flux dédiés sur les réseaux sociaux, complétée par des capteurs techniques collectant des données supplémentaires. Les informations jugées pertinentes ont été classées selon un ensemble de critères, puis analysées et exploitées par les analystes du M-CERT.

Pour cette édition 2025, le suivi des incidents et les statistiques propres au M-CERT sont complétés par des contributions écrites d'organisations partenaires issues de l'écosystème de la cybersécurité maritime — Alcyconie, ATOS, BZHunt, DIATEAM, FMES, GLIMPS, Marlink, Orange Cyberdefense, Semsoft (LESTR) et XRATOR. Chaque section est attribuée à l'organisation qui y a contribué et reflète l'analyse et les points de vue propres à cette organisation.

# 1.

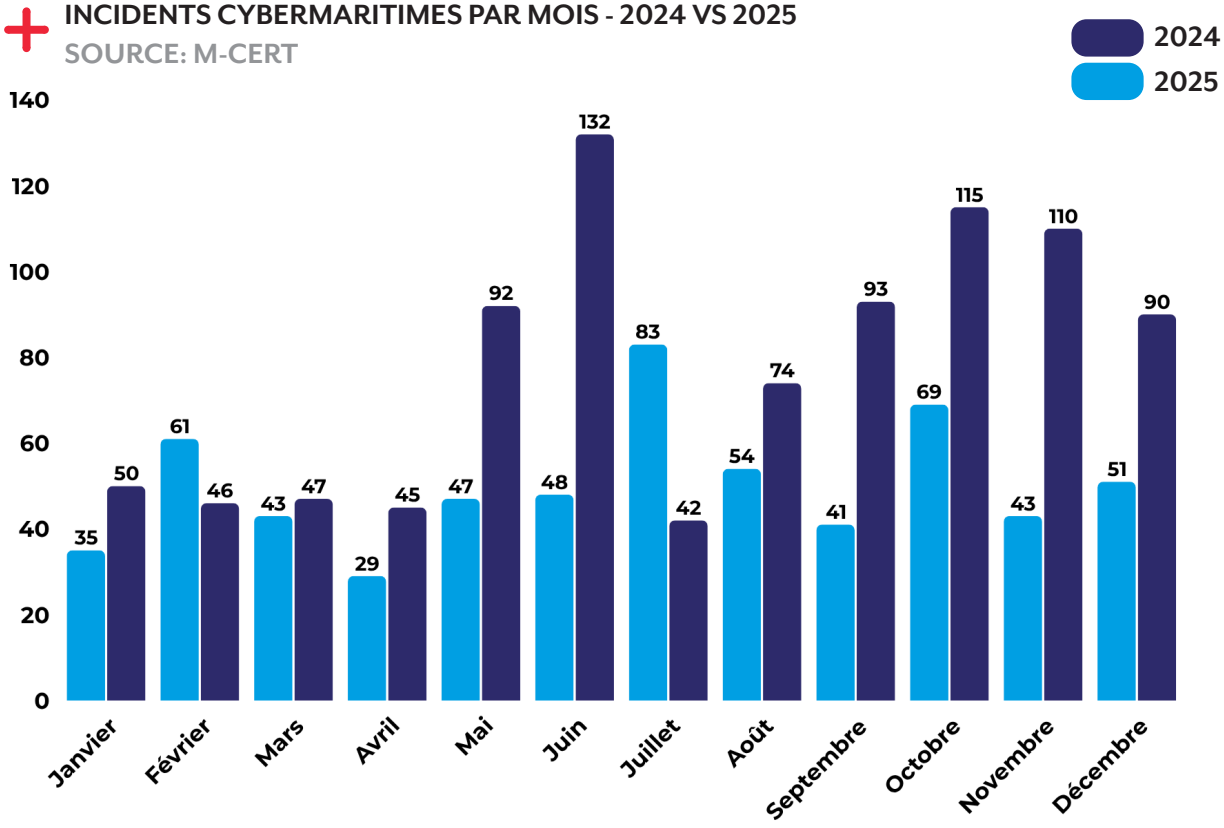
# 2025 EN CHIFFRES

Le M-CERT a recensé les incidents de cybersécurité suivants ayant touché le secteur maritime à l'échelle mondiale en 2024 et 2025 (les noms des victimes n'ont pas été divulgués)

| INDICATEUR | 2024 | 2025 |
|---|---|---|
| Incidents enregistrés | 604 | 936 (+55%) |
| Nombre moyen d'incidents par mois | 50.3 | 78.0 |
| Pays ciblés | 70 | 82 (+90 au total) |
| Part des incidents de type DDoS | 55.3% | 51.6% |
| Part des incidents liés aux ransomwares | 33.0% | 26.1% |
| Part des fuites de données dans les incidents | 7.3% (44) | 17.2% (161, +266%) |
| Part du hacktivisme (type d'acteur) | 61.3% | 53.4% |
| Part de la cybercriminalité (type d'acteur) | 36.9% | 44.7% |
| Incidents commandités par des États (nombre) | 2 | 2 |
| Secteur le plus ciblé | Activité portuaire - 174 incidents | NA |

**INCIDENTS CYBERMARITIMES PAR MOIS - 2024 VS 2025**

SOURCE: M-CERT



## TYPES D'ATTAQUES ET ACTEURS DES MENACES

| CATÉGORIE | 2024 | 2025 |
|---|---|---|
| DDoS | 334 | 483 |
| Ransomware | 199 | 244 |
| Fuite de données | 44 | 161 |
| Autres | 27 | 48 |

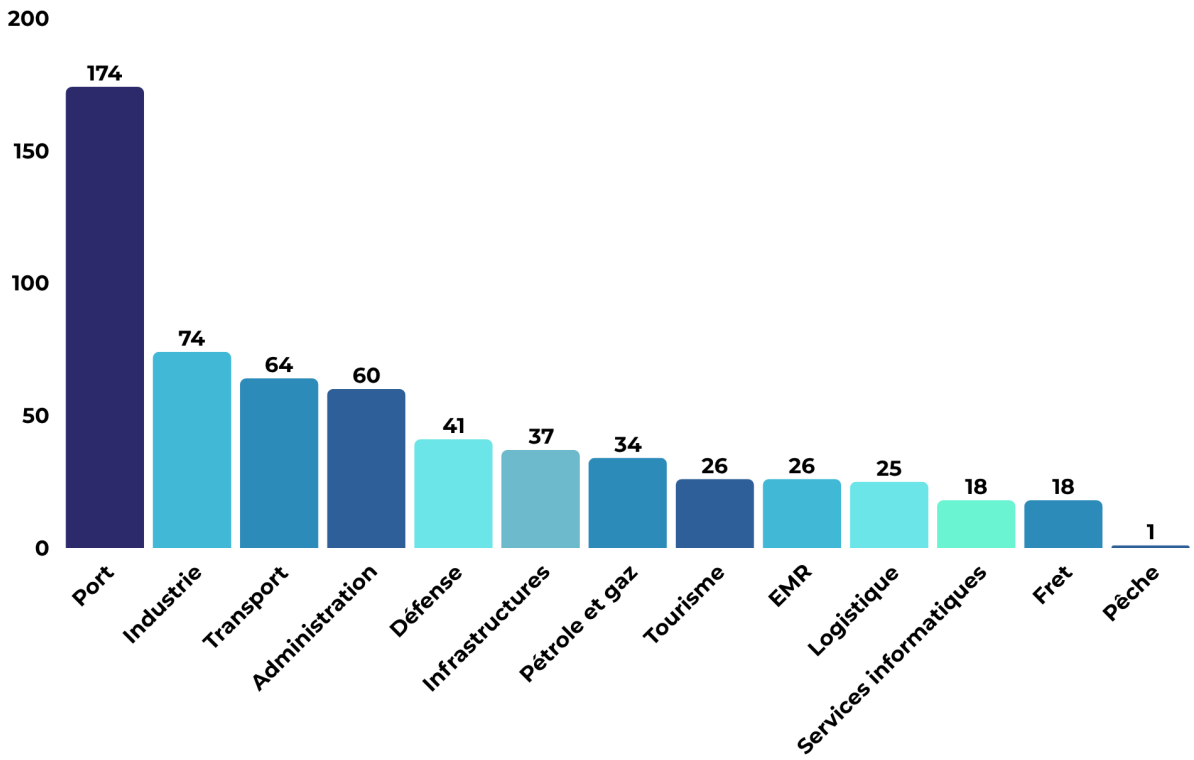
| TYPE D'ACTEURS MALVEILLANTS | 2024 | 2025 |
|---|---|---|
| Hacktivisme | 370 | 500 |
| Cybercriminalité | 223 | 418 |
| Non divulgué | 8 | 16 |
| Étatique | 2 | 2 |

## CLASSIFICATION DES VICTIMES SELON NIS2

| TYPE DE MENACE | 2024 | 2025 |
|---|---|---|
| NC – Non-classé | 50.5% (305) | 61.4% (574) |
| EE/IE – Entité essentielle/importante | 49.5% (278) | 38.7% (334) |

## INCIDENTS PAR SECTEUR MARITIME - 2024

La granularité au niveau sectoriel n'était disponible que pour les données de 2024.



## PRINCIPAUX ACTEURS (HORS CEUX NON DIVULGUÉS)

| CLASSEMENT | 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 |

## TENDANCE CLÉ

**Le nombre d'incidents a bondi de +55 % entre 2024 et 2025. Si les attaques DDoS menées par des hacktivistes restent le type d'attaque dominant, les opérations de cybercriminalité (rançongiciels et fuites de données) gagnent considérablement du terrain : les fuites de données ont à elles seules bondi de de 266 % d'une année sur l'autre. Les États-Unis, Israël, l'Espagne et l'Italie sont systématiquement les pays les plus ciblés.**

## PAYS LES PLUS CIBLÉS (TOP 10)

| CLASSEMENT | 2024 | INCIDENTS | 2025 | INCIDENTS |
|---|---|---|---|---|
| 1 | États-Unis | 108 | États-Unis | 185 |
| 2 | Espagne | 62 | Israël | 96 |
| 3 | Italie | 38 | Italie | 65 |
| 4 | Ukraine | 35 | France | 45 |
| 5 | Allemagne | 27 | Espagne | 43 |
| 6 | Israël | 25 | Royaume-Uni | 33 |
| 7 | Royaume-Uni | 25 | Canada | 26 |
| 8 | Suède | 24 | Thaïlande | 24 |
| 9 | Japon | 24 | Pologne | 24 |
| 10 | France | 20 | Inde | 24 |

# 2.

# LE CONTEXTE GÉOPOLITIQUE


Contribution de la FMES — Fondation Méditerranéenne d'Études Stratégiques, un groupe de réflexion français dédié à la recherche stratégique, à la réflexion et à la formation, à la croisée de la géopolitique, de la défense et de la technologie

# L'ESCALADE DES TENSIONS GÉOPOLITIQUES MARITIMES

**En mer, les rivalités géopolitiques ont tendance à s'exacerber plus rapidement qu'ailleurs. Les zones maritimes sont devenues des lieux où convergent et s'affrontent les intérêts économiques, sécuritaires et de puissance. Le commerce international et la mondialisation ont placé le transport maritime au coeur de l'économie mondiale : il achemine désormais plus de 80% du commerce mondial en volume, rendant les chaînes d'approvisionnement fortement dépendantes des voies maritimes. L'océan abrite également des câbles sous-marins stratégiques ainsi que des ressources halieutiques et minérales très convoitées, ce qui accentue ces tensions.**

L'intensification des rivalités entre grandes puissances (États-Unis, Chine, Russie...) et des conflits régionaux a entraîné une multiplication des zones maritimes de conflit et de tension : de la mer de Chine du Sud au golfe Persique et à la mer Rouge, en passant par la mer Baltique et l'océan Arctique, les acteurs étatiques et non étatiques recourent à toute une gamme de moyens pour poursuivre et défendre leurs intérêts. Loin des zones peuplées, les affrontements en mer ont tendance à prendre des formes débridées et parfois intenses, comme en témoignent la guerre entre la Russie et l'Ukraine en mer Noire, les Houthis en mer Rouge ou les flottes de pêche chinoises en mer de Chine méridionale. Des acteurs privés tels que les armateurs, les exploitants portuaires et les entreprises d'énergie offshore se retrouvent pris dans ces tensions : les navires transportant des matières dangereuses, des marchandises de valeur ou du carburant deviennent des cibles stratégiques et vulnérables.

# LES OPÉRATIONS CYBER, UN OUTIL DE LA GUERRE HYBRIDE

**Les conflits contemporains sont marqués par la guerre hybride, un mélange de méthodes militaires et non conventionnelles qui se situe en deçà du seuil du conflit armé et brouille les frontières du champ de bataille traditionnel. Le cyberespace, invisible et sans frontières, en est le théâtre naturel : sa complexité et l'absence de normes en font un champ de bataille redouté.**

Lorsqu'aucun acteur ne revendique la responsabilité d'un incident, il est difficile de déterminer si une défaillance d'un système informatique résulte d'un dysfonctionnement interne ou d'une ingérence externe. Le piratage informatique est une activité peu coûteuse par rapport aux mesures lourdes nécessaires pour s'en défendre : de petits groupes, tels que les hacktivistes, peuvent provoquer des perturbations numériques à grande échelle contre des concurrents bien plus puissants. Les organisations maritimes, les navires, les systèmes de navigation et les infrastructures portuaires sont la cible de cyberattaques visant à perturber leurs opérations en altérant des données, en retardant les flux de marchandises, voire en provoquant des collisions en rendant les navires indétectables ou en en prenant le contrôle à distance. En 2017, une série de collisions impliquant des navires militaires américains en Asie, dont certaines ont été mortelles, a fait naître des soupçons quant à une éventuelle cyberattaque. Des opérations offensives visant à brouiller le GPS sont de plus en plus signalées dans les régions maritimes, notamment dans le détroit d'Ormuz et le golfe Persique, où transite 20 % du trafic pétrolier mondial et où les interférences GPS entraînent un positionnement peu fiable des navires et des anomalies de l'AIS.

En 2025, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a estimé que les cyberattaques visant tant le secteur public que le secteur privé avaient augmenté de 15 %. CyberOwl, une entreprise spécialisée dans la cybersécurité,

estime qu'une flotte type de 30 navires subit environ 7 cyberattaques par mois, alors que seuls 32 % des armateurs intègrent la cybersécurité au sein de leurs équipes. Or, la prévention des cyberattaques nécessite de nouveaux logiciels de protection et outils défensifs, dont le coût est considérable. Le renforcement de la cyber-résilience exige désormais une coopération plus étroite entre les secteurs public et privé, car les chocs géopolitiques et les menaces hybrides mettent en évidence à quel point l'infrastructure numérique est enréalité interdépendante.

# 4.

# DEUX MENACES, UN SEUL NOM : UNE NOUVELLE PERSPECTIVE SUR LES INCIDENTS MARITIMES EN 2025


Contribution de XRATOR, renseignements et analyse des menaces de cybersécurité

Chaque année, les rapports mondiaux sur la cybersécurité reviennent sur les mêmes thèmes : des ransomwares de plus en plus sophistiqués, des dispositifs d'accès à distance piratés et une inquiétude croissante concernant l'utilisation de l'IA par les cybercriminels. Si l'on examine les incidents maritimes de 2025, ce tableau est incomplet. Les sources ouvertes font état d'une cinquantaine d'événements maritimes notables. Ceux-ci se répartissent en deux catégories qui ont peu de points communs.

La première concerne les ransomwares classiques, motivés par des intérêts financiers : environ seize incidents visant les systèmes informatiques d'intermédiaires maritimes (agences, gestionnaires de navires, chantiers navals, terminaux). Les auteurs n'étaient pas des spécialistes du secteur maritime, mais les mêmes groupes actifs dans tous les secteurs. Qilin apparaît dans cinq cas maritimes, aux côtés d'Akira, de Clop et d'autres. Cela correspond au schéma observé dans les données de l'ENISA et de Verizon pour 2025 : vol de données et double extorsion, les intermédiaires étant pris pour cibles en tant que noeuds de concentration de l'écosystème. Ici, le transport maritime est une cible comme une autre, exposée principalement par l'intermédiaire de ses fournisseurs.

La deuxième famille n'a pas d'équivalent clair à terre, et les rapports axés sur l'informatique la prennent rarement en compte : une vingtaine d'incidents visant les systèmes de positionnement et d'identification (GNSS et AIS). Une partie correspond à des interférences de guerre électronique touchant le trafic civil dans des zones contestées (la Baltique, le détroit d'Ormuz, la mer Rouge, les Caraïbes). Une autre partie consiste en des opérations délibérées de falsification de données de navigation menées par des navires pour contourner les sanctions, documentées par des analystes spécialisés dans le suivi maritime. En nombre d'incidents, cette couche de navigation rivalise avec les ransomwares, mais elle est largement absente des rapports cybernétiques grand public.

Cette distinction est importante car ces deux catégories nécessitent des responsables des risques et des contrôles différents. L'une relève d'un marché criminel visant à obtenir un rançon ; l'autre relève de la géopolitique et de la fraude menées via la couche de radionavigation.

En matière d'intelligence artificielle, les données pour 2025 sont modérées plutôt qu'alarmantes. Aucun des incidents maritimes répertoriés n'a révélé d'attaque pilotée par l'IA. L'utilisation malveillante de l'IA signalée dans divers secteurs par les équipes de surveillance des menaces de Google et d'Anthropic accélère les techniques existantes (hameçonnage, fraude, scripts), mais n'a donné lieu à aucune intrusion autonome ni à aucune hausse marquée, seulement à la poursuite des tendances existantes. L'affaire maritime la plus grave de l'année était de nature physique : les autorités françaises ont découvert un dispositif d'accès à distance installé à bord d'un ferry de passagers par un membre d'équipage agissant pour le compte d'un État étranger. C'est dans le domaine de la défense que l'IA évolue le plus rapidement : tests de sécurité avant la mise en production et tri des alertes.

Ce qui est déjà courant ailleurs et commence seulement à émerger ici, c'est la chaîne d'intrusion standard : identifiants volés, accès négociés, terminaux périphériques exploités. Premiers signes : une agence portuaire desservant des centaines de ports a été compromise via sa chaîne d'approvisionnement, et la compromission d'un fournisseur informatique s'est propagée à une flotte. Cela indique la direction que prend le secteur maritime.

Les responsables de la sécurité, de la sûreté et de la conformité devraient étendre les exigences en matière de cybersécurité et de notification des violations à l'ensemble de la chaîne d'approvisionnement (conformément à la directive NIS2) et inclure dans leur champ d'action les technologies opérationnelles au-delà de la navigation (systèmes de fret, de terminaux et de grues). Les responsables des opérations de flotte et portuaires devraient considérer la navigation sans GNSS fiable comme un risque opérationnel permanent, avec des procédures en mode dégradé et des exercices pour l'équipage ; même si votre propre navire n'est pas brouillé, un autre croisant votre route pourrait l'être. Les décideurs devraient financer ces deux volets séparément : l'exposition aux ransomwares est similaire à celle de tous les autres secteurs, tandis que la résilience en matière de positionnement est spécifique au secteur maritime. Les solutions existent ; l'année 2025 a simplement montré celles que le secteur considère encore comme le problème de quelqu'un d'autre.

# 5.

# ZOOM SUR LE SECTEUR PORTUAIRE : RÉPÉTER LE SCÉNARIO DE L'ATTAQUANT

Contribution from DIATEAM,
une société Cy4gate,
Amélie GAUTIER, ingénieure commerciale

DIATEAM Maritime Hybrid Cyber Range

**Fondée en 2002, DIATEAM est un leader mondial sur le marché des cyber-centres d'entraînement hybrides et du prototypage d'infrastructures numériques, avec une spécialisation particulière dans le secteur maritime. Ses missions sont les suivantes : la formation à la cybersécurité des professionnels des secteurs maritime et portuaire à l'aide de simulations réalistes couvrant à la fois les environnements informatiques (IT) et opérationnels (OT) ; la simulation de pointe d'adversaires soutenus par des États ou de cybercriminels dans un contexte maritime ; et la fourniture de cyber-pistes hybrides destinées à servir de plateformes de jumeaux numériques et de prototypage.**

# CYBERATTAQUES CONTRE LES PORTS EUROPÉENS EN 2025

En février 2025, une intrusion a mis hors service le système communautaire portuaire (PCS) d'un port de la mer du Nord – qui enregistre les mouvements des navires, les listes d'équipage et les flux de marchandises. Les TTP observées lors des opérations de ransomware maritime affectant l'écosystème portuaire au sens large en 2025 suivaient un schéma récurrent : exploitation des appliances de cybersécurité en périphérie, réutilisation d'identifiants issus de journaux d'infostealers vendus par des courtiers en accès initial, spear-phishing visant les équipes financières et logistiques, et pivots via des MSP compromis.

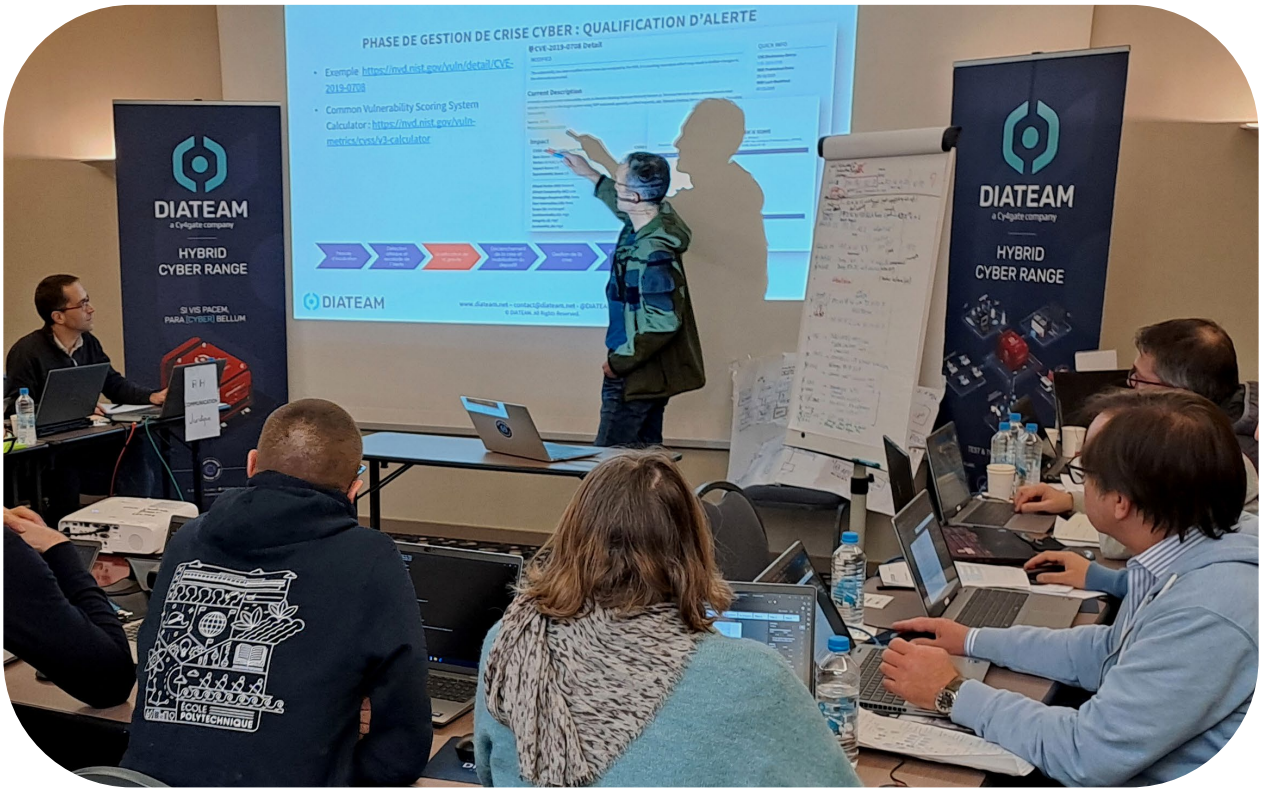
La veille open source a recensé 149 incidents cybernétiques dans le secteur portuaire en 2025, en grande majorité des attaques DDoS (132 cas, soit 88,6 %), menées par le collectif pro-russe NoName057(16) et concentrées sur l'Italie (47 cas, près d'un tiers du total), la Pologne, la Finlande, l'Espagne, la Belgique et la Lituanie – dans la continuité de la stratégie hybride mise en place après 2022 contre les membres de l'OTAN. Les attaques directes par ransomware contre les autorités portuaires ont été rares (8 cas, dont un seul dans l'UE) ; c'est l'écosystème maritime au sens large, en amont des opérations portuaires – compagnies maritimes, agences, fabricants d'équipements, fournisseurs de logiciels – qui a absorbé l'essentiel de l'activité liée aux ransomwares, avec 18 attaques de ce type visant la logistique. L'impact des hacktivistes reste limité tandis que les attaques DDoS se concentrent sur les sites marketing ; le PCS national italien a été touché lors de dix campagnes depuis 2023, dont quatre rien qu'en 2025, parallèlement à des vagues d'attaques sur l'Adriatique et les Autorités portuaires de la mer Tyrrhénienne.

Les dépendances externes définissent la véritable surface d'attaque. Un éditeur de logiciels américain au service d'opérateurs portuaires a été compromis en septembre, exposant ainsi ses clients en aval : accès d'apparence légitime de MSP, de fournisseurs de cloud, de bibliothèques
tierces non mises à jour et d'initiés, avec moins de signaux de détection. Sur la côte baltique, une guerre électronique soutenue a rendu le positionnement GPS indisponible environ 17 % du temps pendant les mois de pointe de 2025 ; des données AIS falsifiées et un positionnement dégradé sapent la conscience situationnelle des VTS et des pilotes au moment où cela compte le plus.

Au sein des terminaux à conteneurs, la convergence entre IT, OT, IoT et 5G crée des voies latérales que la segmentation conventionnelle parvient rarement à contenir ; le périmètre RF (Wi-Fi, 5G privée, IoT, AIS, GNSS) et les vecteurs physiques (USB, clonage de badges, appareils de terrain) étendent la surface que la plupart des ports ne cartographient pas. L'IA réduit le coût de production des attaques de type BEC et accélère la découverte des vulnérabilités des systèmes portuaires exposés.

Pour combler cette lacune, il faut s'entraîner à reproduire les modes opératoires des attaquants : des campagnes adversaires menées sur la durée, déployées sur l'ensemble du périmètre étendu – opérateurs de terminaux, prestataires informatiques, sous-traitants logistiques – afin de tester la détection, la prise de décision et la résilience dans des conditions de pression réalistes. DIATEAM a développé cette capacité pour le secteur maritime depuis plus d'une décennie, en combinant des opérations de « red team » avec un cyber-centre

d'entraînement hybride qui reproduit fidèlement les systèmes réels des navires et des ports (ECDIS, AIS, GPS, SATCOM, OT). « Nous ne vendons pas d'outils cybernétiques ; nous affinons la manière dont vos équipes utilisent ceux dont vous disposez déjà. Si vous exploitez un port et souhaitez voir votre surface d'attaque à travers les yeux d'un adversaire déterminé, contactez-nous. »




DIATEAM Hybrid Cyber Range crisis-management exercise

# 6.

# LES SYSTÈMES OT DANS L'OEIL DU CYCLONE

Contribution d'Orange Cyberdefense, Ludovic JAMART, Directeur Conseil et Audit Grand Ouest, Orange Cyberdefense France

**L'année 2025 a démontré que le secteur maritime et portuaire ne peut plus ignorer la cybermenace. Des études indiquent un doublement des cyberattaques ciblant ce secteur en 2025, visant en particulier les équipements OT (technologies opérationnelles) — matériel et logiciels qui contrôlent directement les fonctions critiques des navires et des infrastructures portuaires, de plus en plus exposés en raison de la convergence accélérée entre l'informatique et les technologies opérationnelles (IT/OT) et de l'extension de la connectivité entre la terre et la mer.**

## PARMI LES INCIDENTS LES PLUS MARQUANTS

**La cyberattaque contre Fanava**, le fournisseur iranien de services VSAT, a eu lieu en mars et en août 2025. Attribuée au groupe hacktiviste iranien Lab Dookhtegan, elle a paralysé les communications à terre de plus de 150 navires des flottes de la National Iranian Tanker Company et de l'Islamic Republic of Iran Shipping Lines. L'attaque a suivi un schéma classique de la chaîne d'approvisionnement : intrusion dans le centre terrestre de Fanava pour atteindre la flotte connectée, accès administrateur aux terminaux VSAT, et désactivation du service satellite iDirect Falcon — coupant ainsi les liaisons navire-terre et paralysant les transpondeurs AIS. Une dernière technique d'effacement a permis de supprimer les données et les journaux des terminaux, immobilisant les navires pendant plusieurs semaines en attendant une réinstallation manuelle.

**L'échouage du MSC Antonia** en mai 2025 sur les récifs coralliens d'Eliza Shoals, en mer Rouge, illustre les dommages collatéraux subis par les acteurs du transport maritime à proximité des zones de conflit armé. Alors qu'il faisait route vers Djeddah, le MSC Antonia est entré dans une « bulle de spoofing » : ses récepteurs GNSS ont capté de faux signaux qui ont désorienté les instruments de navigation (AIS, ECDIS), affichant une position erronée — avec des écarts de plus de 6 000 km — et rendant impossible le recalcul de la trajectoire. De nuit, en l'absence de repères visuels fiables, l'équipage n'a pas pu éviter l'échouage. Cet incident, qui n'a fait ni victime ni pollution, met en évidence le danger d'une confiance aveugle dans les outils de navigation numériques et le manque de cyber-résilience des systèmes embarqués.

**Les campagnes menées par le groupe de cyberattaques russe APT28** (également connu sous le nom de Fancy Bear) visaient les infrastructures logistiques et portuaires de plusieurs pays de l'OTAN soutenant l'Ukraine, notamment Hambourg et Rotterdam. D'après les connaissances actuelles, ces campagnes ont principalement permis la reconnaissance et le prépositionnement, en s'appuyant sur des attaques par force brute, le vol d'identifiants, le spear-phishing (documents de transport ou douaniers falsifiés) ciblant des utilisateurs clés de l'écosystème portuaire, l'exploitation de vulnérabilités connues et l'utilisation abusive de services cloud ou de logiciels légitimes pour maintenir une persistance indétectable. Les objectifs consistent à collecter des informations sur les cargaisons, les dates et les itinéraires de l'aide logistique et militaire transitant par les ports, ainsi qu'à accéder aux systèmes de caméras IP ou aux passerelles informatiques/opérationnelles (IT/OT) afin de prendre potentiellement le contrôle des systèmes de gestion des terminaux portuaires. À ce jour, aucun acte de sabotage n'a été observé.

## UNE RÉPONSE RÉGLEMENTAIRE SE MET EN PLACE

Les autorités maritimes internationales réagissent. Le 4 avril 2025, l'OMI a publié la révision n° 3 de la circulaire MSC-FAL.1/Circ.3 relative aux lignes directrices sur la gestion des risques cybermaritimes, renforçant le cadre réglementaire en :

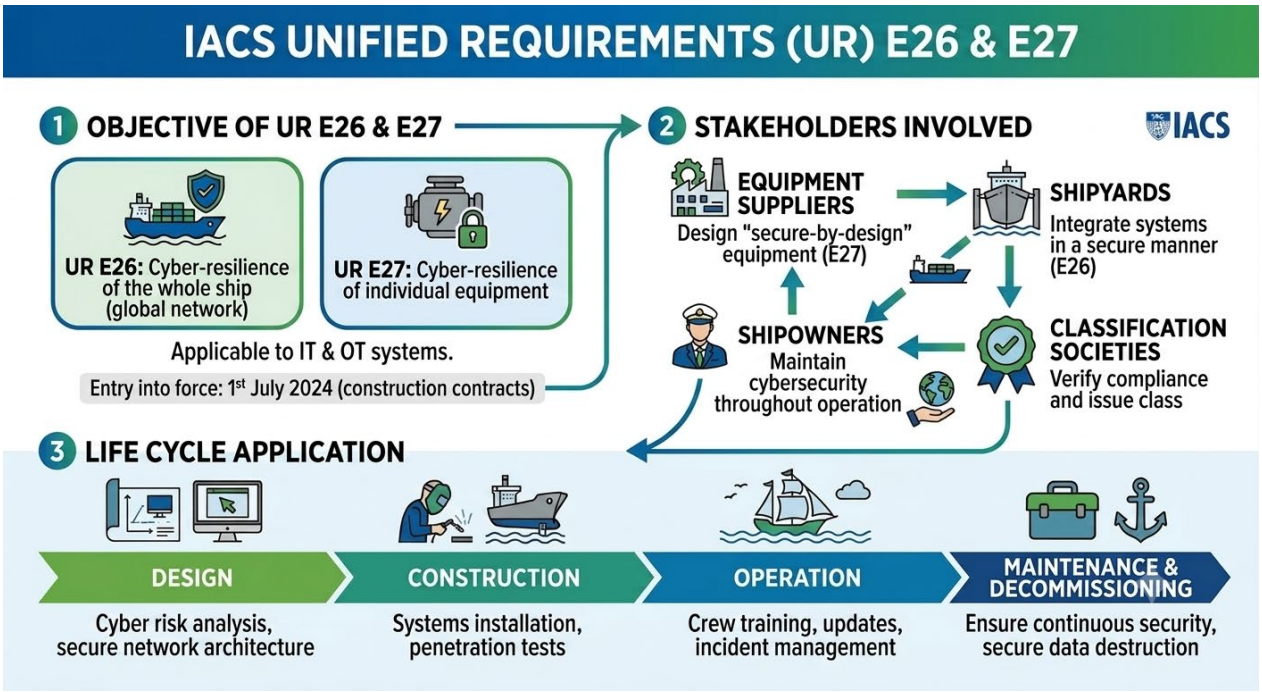
- Ajoutant la fonction « Gouverner » au processus de gestion des risques, ce qui implique la désignation d'un responsable de la cybersécurité

doté des ressources, de l'autorité et du soutien nécessaires à l'exercice de ses fonctions.

- Attirant l'attention sur les systèmes OT et les risques liés aux tiers.

Malgré ces avancées, la circulaire de l'OMI reste non contraignante en droit international. Les progrès les plus notables concernant un cadre de cybersécurité maritime proviennent de l'IACS (Association internationale de classification), qui a introduit les exigences unifiées (UR) E26 et E27 relatives à la cyber-résilience des systèmes et équipements embarqués. Celles-ci sont devenues obligatoires pour tous les nouveaux navires commandés après le 1er juillet 2024, couvrant l'ensemble des systèmes informatiques (IT) et opérationnels (OT) tout au long du cycle de vie du navire — conception, construction et exploitation — pour tous les navires classés de plus de 500 GT effectuant des voyages internationaux. Une majorité des sociétés de classification membres de l'IACS ont aligné leur notation de classe sur les UR E26 et E27.

Première étape vers le Maritime security by design.




Orange Cyberdefense est la filiale du groupe Orange spécialisée dans la cybersécurité. Forte de plus de 3 300 experts répartis dans 12 pays et de 36 centres de détection à travers le monde, elle contribue à bâtir une société numérique plus sûre en accompagnant les organisations tout au long du cycle de vie des cybermenaces : anticipation, détection, réponse aux incidents et sécurisation des systèmes informatiques et OT critiques.

# 7.

# LA LIAISON MER-CÔTE : UNE NOUVELLE FRONTIÈRE


Contribution de Marlink, connectivité maritime et renseignements sur les cybermenaces

# SURFACE D'ATTAQUE ET VECTEURS CLÉS

En 2025, la liaison mer-terre — terminaux de communication par satellite, plateformes d'accès à distance, systèmes informatiques de la flotte, données AIS/GNSS, canaux d'escale et systèmes informatiques/opérationnels à terre — est devenue la zone la plus vulnérable sur le plan stratégique de l'environnement opérationnel maritime. La menace principale n'est plus la compromission de navires individuels, mais les attaques visant la chaîne d'approvisionnement au niveau des fournisseurs et des équipementiers, susceptibles d'affecter des flottes entières. Le nombre d'incidents cybernétiques maritimes signalés a augmenté d'environ 100 % d'une année sur l'autre (données CYTUR/SAFETY4SEA), et leurs conséquences sont passées principalement du vol à davantage de déni de service, de destruction et de risques pour la sécurité physique.

# LES PRINCIPAUX CONSTATS

- Les ransomwares et la double extorsion visant les réseaux à terre, les fournisseurs et les voies d'accès à distance constituent la catégorie d'incidents merterre la plus fréquente en 2025.
- La compromission de la chaîne d'approvisionnement des fournisseurs de communications par satellite et de logiciels constitue le vecteur aux conséquences les plus graves : un seul point d'ancrage permet d'affecter l'ensemble d'une flotte.
- Les interférences GNSS/AIS dans les eaux contestées (détroit d'Ormuz, mer Rouge, mer Noire) constituent désormais un risque cyber-physique opérationnel persistant.
- Les acteurs liés à des États continuent de représenter la menace aux conséquences les plus graves par le biais de l'espionnage et du prépositionnement
- La dynamique réglementaire (règle MTS de l'USCG, OMI, IACS) rehaussera le niveau de référence, mais ne comblera pas les lacunes en matière d'exposition dès 2025, compte tenu des calendriers échelonnés et des contraintes liées aux systèmes hérités.

# ACTEURS MENAÇANTS

Quatre catégories d'acteurs mènent des actions contre la liaison mer-terre, différenciées par leurs intentions et leurs conséquences :

**Acteurs étatiques et liés à des États** : la menace aux conséquences les plus graves. Mustang Panda (Chine) a ciblé des entreprises de transport maritime de fret en Norvège, en Grèce et aux Pays-Bas ; APT41 a frappé les secteurs du transport maritime et de la logistique au Royaume-Uni, en Italie, en Espagne, en Turquie, à Taïwan et en Thaïlande ; Crimson Sandstorm, lié à l'Iran, a ciblé des opérateurs maritimes de la Méditerranée ; Turla/Tomiris et RedCurl, liés à la Russie, ont mené des opérations d'espionnage industriel contre des cibles des secteurs du transport et de la logistique. L'accès ainsi établi permet ensuite d'exercer une pression ou de provoquer des perturbations.

**Groupes criminels organisés** : les perturbateurs les plus courants. Les ransomwares de double extorsion combinent le chiffrement et les menaces de vol de données, ciblant les prestataires à terre et les appareils d'accès à distance exposés. La motivation est financière, mais les conséquences opérationnelles sont indissociables d'une perturbation délibérée.

**Les hacktivistes** : généralement limités aux attaques DDoS et aux fuites, mais l'opération Lab Dookhtegan / Fanava (voir également la section « Systèmes OT » dans ce rapport) a démontré une portée à l'échelle de la flotte via la compromission d'un fournisseur de communications par satellite, brouillant ainsi la frontière avec les opérations destructrices relevant de l'État.

**Initiés et sous-traitants** : ils conservent un avantage structurel grâce à leur accès autorisé. Dans un écosystème fortement externalisé, le périmètre des initiés s'étend aux fournisseurs de services gérés et de communications par satellite, comme le montre l'affaire Ferry Fantastic.

# VULNERABILITÉS STRUCTURELLES

Les systèmes critiques pour la sécurité hautement connectés — notamment ceux reliés à des fournisseurs à terre, à des liaisons satellitaires ou utilisant des identifiants partagés — sont les plus exposés. Deux vulnérabilités structurelles se distinguent :

**Le terminal de communication par satellite comme point de défaillance unique** : bon nombre de ces appareils ont été conçus pour la connectivité, et non pour la résilience. La compromission d'un terminal permet à l'adversaire de prendre le contrôle de toutes les communications du navire et de s'introduire dans les systèmes informatiques embarqués et, dans les environnements mal segmentés, dans les systèmes OT.

**Concentration des fournisseurs** : les opérateurs de communications par satellite, les intégrateurs informatiques gérés, les éditeurs de logiciels et les serveurs de mise à jour concentrent les risques — une seule compromission peut se propager simultanément à de nombreux navires ou terminaux.

# PRINCIPAUX VECTEURS D'ATTAQUE EN 2025

**Hameçonnage et vol d'identifiants** : 43 % des incidents cybernétiques MTS signalés à l'USCG en 2025 ont utilisé l'hameçonnage pour l'accès initial (contre 25 % en 2024) ; les comptes compromis ont été utilisés comme armes pour des campagnes ultérieures.

**Chaîne d'approvisionnement / tiers** : les cas de DNV ShipManager, Furuno et Lab Dookhtegan / Fanava illustrent deux niveaux — compromission de la plateforme SaaS et compromission de l'équipementier (OEM) — tous deux ayant une portée à l'échelle de la flotte. Appareils d'accès à distance : VPN exposés, RDP et interfaces de gestion (y compris les CVE de Citrix NetScaler) utilisés comme vecteurs d'accès initial.

**Supports amovibles et acteurs internes** : des infections par clé USB ont été documentées dans le cadre des campagnes Turla/Tomiris et de l'intrusion « Ferry Fantastic ».

**Manipulation des systèmes PNT** : brouillage et usurpation GNSS endémiques dans le détroit d'Ormuz, la mer Rouge et la mer Noire ; effets en cascade sur les systèmes ECDIS, AIS, les gyroscopes, les systèmes anticollision et la planification des arrivées dans les ports.

Maritime SOC monitoring global fleet connectivity — Source: Marlink

Extrait de Marlink CTI — « Aperçu des menaces et des attaques visant la liaison mer-terre ».
Contact : cti@marlink.com

# 8.

# ZOOM : L'USURPATION D'IDENTITÉ AIS, DE LA DISPARITION À LA TROMPERIE

Contribution de Semsoft (LESTR), fusion de données et IA pour la détection des risques liés au commerce maritime

**Semsoft, une entreprise technologique française spécialisée dans la fusion de données et l'intelligence artificielle, a développé LESTR (mot breton signifiant « navire » et acronyme de « Limit your Exposure to Sanctions and other Trade Risks », soit « Limitez votre exposition aux sanctions et autres risques commerciaux »), un outil qui détecte les activités illicites dissimulées au sein du commerce maritime et des opérations de fret légitimes.**

Pendant des décennies, les opérateurs maritimes illicites poursuivaient un objectif simple : éviter d'être repérés. Au départ, la dissimulation était essentiellement physique : il suffisait souvent de changer le nom, l'apparence ou le pavillon d'un navire.

L'adoption généralisée du système d'identification automatique (AIS), combinée à la surveillance par satellite, a transformé la manière dont les navires pouvaient être suivis. L'activité maritime est devenue transparente, offrant aux acteurs de la sécurité une visibilité sans précédent sur les mouvements des navires.

À mesure que la transparence s'accroissait, les opérateurs se sont adaptés : plutôt que de se dissimuler physiquement, de nombreux navires ont simplement cessé d'émettre. Ces interruptions volontaires de l'AIS sont rapidement devenues l'un des signes les plus évidents de contournement des sanctions, de transferts illicites de navire à navire (STS) et de contournement d'embargo.

Mais cette stratégie a été victime de son propre succès : aujourd'hui, une interruption inexpliquée de l'AIS suffit souvent à elle seule à déclencher une enquête. Dans de nombreux cas, disparaître est devenu plus suspect que de rester visible.

Les pratiques d'évasion maritime sont devenues nettement plus sophistiquées. Au lieu de disparaître, les navires restent désormais de plus en plus souvent visibles tout en diffusant de fausses informations — une pratique connue sous le nom de « spoofing AIS », qui consiste à altérer délibérément les données afin de dissimuler la véritable identité ou la position d'un navire et de masquer des activités illicites.

Les premières tentatives de falsification étaient souvent rudimentaires. Les analystes observaient parfois des navires opérant dans des lieux impossibles ou diffusant des identifiants manifestement faux ; ces anomalies étaient relativement faciles à détecter.

L'usurpation d'identité est devenue bien plus sophistiquée. Les stratagèmes de base consistent à transmettre de faux noms de navires, numéros MMSI, indicatifs d'appel ou numéros OMI — une tactique observée depuis longtemps dans le cadre du contournement des sanctions contre la Corée du Nord, comme dans le cas du pétrolier An San 1. Des opérations plus avancées, parfois appelées « blanchiment d'identité de navire », consistent à s'approprier l'identité d'un navire légitime pour servir de couverture à un navire se livrant à des activités illicites : l'objectif n'est plus de se cacher, mais de devenir quelqu'un d'autre.

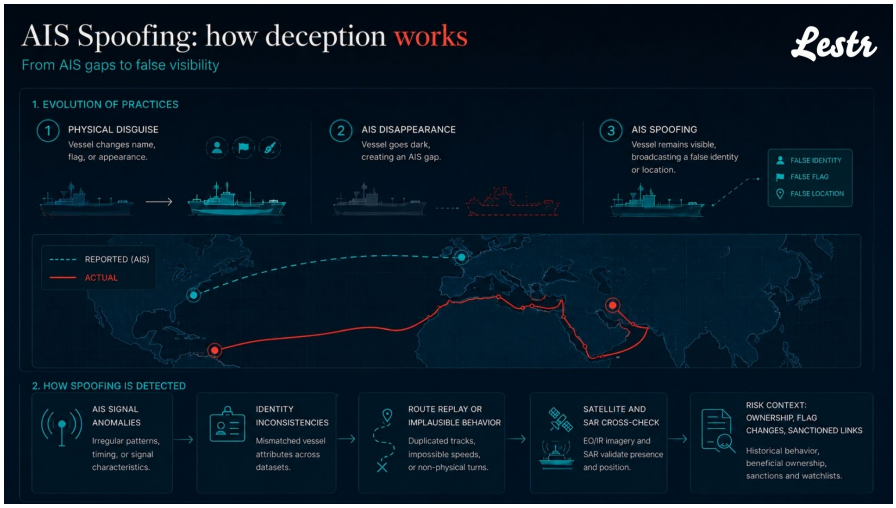
La localisation évolue de la même manière. Plutôt que de générer des trajectoires impossibles, les opérateurs rejouent désormais des séquences AIS historiques légitimes, de sorte qu'un analyste s'appuyant uniquement sur l'AIS voit un itinéraire plausible alors que l'activité réelle du navire se déroule ailleurs. Ce phénomène a été observé avec le méthanier IMO 9307205, qui a diffusé une fausse position dans les eaux malaisiennes afin de masquer sa présence aux côtés d'un navire sanctionné lors d'un transfert clandestin de gaz russe de navire à navire — un comportement qui a contribué à son inscription sur la liste noire des autorités britanniques.

Cette évolution reflète la réalité géopolitique actuelle. Le durcissement des sanctions contre la Russie, l'Iran et la Corée du Nord a créé de fortes incitations à dissimuler les flux énergétiques illicites, accélérant ainsi le développement de stratagèmes de tromperie maritime de plus en plus sophistiqués.

La détection de telles pratiques nécessite de combiner plusieurs sources de preuves. L'analyse moderne s'appuie sur des approches «signal-first» pour analyser les messages AIS à la recherche d'incohérences et d'anomalies. Parallèlement, les approches «image-first» permettent de comparer les positions signalées par l'AIS avec l'imagerie satellite et les observations SAR. De plus en plus, le renseignement sur les radiofréquences offre un moyen indépendant de confirmer la présence d'un navire, même lorsque les données AIS ont été manipulées.

Cependant, l'usurpation d'identité ne doit pas être considérée comme un indicateur isolé. Les navires se livrant à des manoeuvres de dissimulation sophistiquées présentent souvent d'autres caractéristiques à haut risque, notamment l'absence d'assurance P&I, des antécédents de non-conformité lors des inspections de contrôle par l'État du port et des changements fréquents de nom ou de pavillon.

En fin de compte, le défi dépasse le cadre de l'AIS lui-même. L'enjeu réside dans la fiabilité des informations utilisées pour surveiller et sécuriser les activités maritimes. Aujourd'hui, les navires qui nous préoccupent le plus ne sont souvent pas ceux qui se font discrets, mais ceux qui restent visibles tout en diffusant une fausse réalité.




Évolution des pratiques de contournement — camouflage physique, disparition de l'AIS et usurpation de l'AIS — et comment les analystes les détectent : anomalies de signal, incohérences d'identité, relecture d'itinéraire, recoupements satellite/SAR et analyse du contexte de risque.
Source : LESTR / Semsoft

# 9.

# PRINCIPALES VULNÉRABILITÉS EXPLOITÉES EN 2025 ET TENDANCES

Contribution de GLIMPS, analyse approfondie de fichiers et caractérisation des logiciels malveillants grâce à l'IA

**En 2025, la France est confrontée à une forte augmentation des incidents de cybersécurité et des violations de données. Plus de 6 000 déclarations de violations de données à caractère personnel ont été déposées auprès de la CNIL, un niveau historiquement élevé touchant tous les secteurs : administration publique, santé, éducation, industrie, services financiers et grandes plateformes numériques. Les enjeux financiers et de réputation ne cessent de croître.**

**Cette recrudescence des violations rappelle l'importance de rester vigilant face au phishing et à l'ingénierie sociale. Les campagnes deviennent de plus en plus convaincantes, notamment grâce à l'IA, qui génère à grande échelle des e-mails, des sites web frauduleux et des messages très crédibles, dans toutes les langues européennes.**

Dans le même temps, on observe une légère baisse des attaques par ransomware a été observée, bien qu'elle reste relative : les groupes criminels adaptent leurs méthodes plutôt que de disparaître. Parmi les plus actifs : Qilin, Akira, Cl0p, Play et LockBit. Les opérateurs se montrent de plus en plus agressifs. Le chiffrement n'est plus systématique, tandis que le vol massif de données, les menaces de divulgation et les pressions exercées sur les partenaires et les clients sont devenus les leviers privilégiés. Associé à l'IA, cela laisse présager des campagnes encore plus sophistiquées à l'avenir.

Les outils d'administration légitimes ont toujours été présents dans les chaînes d'attaque, mais leur utilisation est devenue quasi systématique. Les attaquants privilégient des outils connus et de confiance pour se fondre dans l'activité normale du système ou exploiter des versions vulnérables, ce qui rend les activités malveillantes bien plus difficiles à détecter et à bloquer. Deux perspectives complémentaires se dégagent.

En termes de gravité, le CERT-FR n'a émis que trois alertes de niveau maximal au cours de l'année, toutes ciblant des infrastructures largement déployées : Citrix NetScaler (CVE-2025-7775, exécution de code à distance), Cisco ASA/FTD VPN (CVE-2025-20333/20362) et React Server Components (CVE-2025-55182, exécution de code à distance sans authentification) ; Fortinet FortiWeb (CVE-2025-64446) a été signalé comme faisant l'objet d'une exploitation active.

Si l'on se base sur le volume de signalements (issus des avis de sécurité et de la couverture médiatique, un indicateur de l'impact réel), le classement évolue : React RSC (CVE-2025-55182) arrive en tête de liste, devant la faille zero-day d'Oracle E-Business Suite exploitée par Cl0p (CVE-2025-61882), Fortra GoAnywhere MFT (CVE-
2025-10035, CVSS 10,0), et la chaîne « ToolShell » de Microsoft SharePoint (CVE- 2025-53770/53771).

Le point commun : des terminaux en périphérie exposés, des serveurs de transfert de fichiers et de collaboration, exploités via des failles « zero-day » quelques jours seulement après leur divulgation. La priorité en matière de défense est claire : appliquer rapidement les correctifs sur les systèmes périphériques et surveiller les accès à distance.

# VULNÉRABILITÉS: GRAVITÉ ET SIGNALEMENT

Deux perspectives complémentaires se dégagent.

**En termes de gravité**, le CERT-FR n'a émis que trois alertes de niveau maximal au cours de l'année, toutes ciblant des infrastructures largement déployées : Citrix NetScaler (CVE-2025-7775, exécution de code à distance), Cisco ASA/FTD VPN (CVE-2025-20333/20362) et React Server Components (CVE-2025-55182, exécution de code à distance sans authentification) ; Fortinet FortiWeb (CVE-2025-64446) a été signalé comme faisant l'objet d'une exploitation active.

**Si l'on se base sur le volume de signalements** (issus des avis de sécurité et de la couverture médiatique, un indicateur de l'impact réel), le classement évolue : React RSC (CVE-2025-55182) arrive en tête de liste, devant la faille zero-day d'Oracle E-Business Suite exploitée par Cl0p (CVE-2025-61882), Fortra GoAnywhere MFT (CVE- 2025-10035, CVSS 10,0), et la chaîne « ToolShell » de Microsoft SharePoint (CVE- 2025-53770/53771).

Le point commun : des terminaux en périphérie exposés, des serveurs de transfert de fichiers et de collaboration, exploités via des failles « zero-day » quelques jours seulement après leur divulgation. La priorité en matière de défense est claire : appliquer rapidement les correctifs sur les systèmes périphériques et surveiller les accès à distance.

## LE RÔLE DE L'IA

En 2025, l'IA est passée du stade des premières expérimentations à celui d'outils industrialisés couvrant l'ensemble de la chaîne d'attaque :

**Automatisation du phishing :** oui, et généralisée. Génération massive d'appâts, de faux sites et de messages multilingues très convaincants.

**Recherche de vulnérabilités** : émergente. L'IA facilite la révision et le triage du code pour détecter plus rapidement les failles, même si l'expertise humaine reste déterminante.

**Génération de scripts d'exploitation** : émergente. L'IA aide à rédiger et à adapter le code de preuve de concept et les exploits, abaissant ainsi la barrière à l'entrée.

## PERSPECTIVES

Le scénario pour 2025 est celui d'une convergence : une exploitation plus rapide des vulnérabilités du périmètre, des intrusions plus furtives via des outils de confiance, et un arsenal offensif renforcé par l'IA. Cependant, cette même technologie renforce la défense, en accélérant la détection, le triage et la réponse pour les organisations qui l'adoptent rapidement.


Top 10 vulnerabilities by volume of reports, 2025

# 10.

# LE VIRAGE : LES CYBERATTAQUES BASÉES SUR L'IA ET CE QUE LE SECTEUR MARITIME DOIT SURVEILLER

Contribution de BZHunt, cybersécurité offensive, tests d'intrusion et exercices de simulation d'attaques (« red teaming »)

**BZHunt est une société française de cybersécurité offensive basée en Bretagne, spécialisée dans les tests d'intrusion, les exercices de simulation d'attaques (red teaming) et les audits de sécurité des infrastructures maritimes et portuaires. Ses équipes allient une expérience acquise dans le domaine des programmes de prime aux bogues à une expertise de terrain pour aider les opérateurs à anticiper les menaces plutôt que d'y réagir.**

**Tout capitaine sait que le véritable danger réside rarement dans la vague que l'on voit arriver — c'est la houle sous la surface, le courant qui change imperceptiblement jusqu'à ce que la coque dévie de sa trajectoire. Il en va désormais de même en matière de cybersécurité : derrière les gros titres sur les paralysies causées par les ransomwares, un changement plus discret est en cours — l'IA fait son entrée dans la panoplie des attaquants.**

## UN CHANGEMENT DE CONTEXTE, PAS ENCORE UN CHANGEMENT DE NATURE

La tentation, alimentée par le marketing des fournisseurs, est d'imaginer que l'IA va faire apparaître des catégories d'attaques entièrement nouvelles. La réalité est plus sobre : lorsque Anthropic a présenté son modèle Mythos comme capable de découvrir de manière autonome des vulnérabilités au niveau du noyau, les chercheurs de Rival Security ont constaté que le cas phare, CVE-2026-4747 dans FreeBSD, était une réplique presque identique de CVE-2007-3999, un débordement corrigé dans MIT Kerberos deux décennies plus tôt et probablement présent dans les données d'entraînement du modèle. Mythos n'a rien inventé ; il a reconnu, recombiné et exploité à la vitesse d'une machine. Daniel Stenberg, créateur de cURL, est parvenu à une conclusion similaire après que Mythos eut analysé son projet : sur les cinq vulnérabilités signalées, seule une faille de faible gravité s'est avérée fondée. Dans The Register, il a estimé que le discours sur cette avancée était « avant tout du marketing » et que les outils d'IA actuels détectaient « le type d'erreurs habituelles et bien connues que nous connaissons déjà. Ils ne font que trouver de nouveaux exemples de celles-ci. »

## POURQUOI LES PORTS SONT-ILS LES ENDROITS LES PLUS EXPOSÉS ?

Pour une autorité portuaire ou un opérateur de terminal, cette nuance ne réduit pas le niveau de menace — elle l'augmente. L'exposition n'est plus théorique : depuis 1980, 542 incidents cybernétiques rendus publics ont touché des ports à travers le monde, tandis que 117 autres ont affecté la chaîne logistique au sens large. Les ports sont, de loin, le noeud le plus ciblé de l'écosystème maritime.

Il convient ici de distinguer deux surfaces d'attaque très différentes. Les armateurs doivent composer avec l'AIS, l'ECDIS et les systèmes de navigation embarqués ; les ports sont confrontés à un environnement plus complexe : des systèmes interconnectés (PCS, CCS, TOS), des services de trafic maritime consommant les flux AIS sans en émettre, des contrôleurs industriels sur les grues et les portails, des capteurs IoT répartis sur les quais, et de plus en plus de réseaux 5G privés — et la plupart des opérateurs ont également transféré une grande partie de leur infrastructure informatique vers des clouds publics, élargissant ainsi la surface d'attaque.

Ce sont précisément ces environnements où sommeillent des vulnérabilités oubliées, et où un assistant IA entre les mains d'un attaquant devient redoutable — non pas un génie, mais un analyseur de correspondances infatigable qui passe au crible le code plus rapidement que n'importe quelle équipe rouge humaine, dénichant les recoins où des bogues datant de 2007 ont été discrètement copiés dans des systèmes de 2026. Tout opérateur portuaire sérieux

devrait partir du principe qu'il est constamment scruté, et qu'un attaquant a probablement déjà trouvé des points d'ancrage, attendant le moment propice.

Comme l'a fait remarquer Matthew Rosenquist, stratège en cybersécurité, les attaquants disposent d'un avantage structurel : ils peuvent adopter immédiatement des outils d'IA non vérifiés et risqués, sans assumer aucune responsabilité pour les dommages collatéraux — ce que les défenseurs ne peuvent pas faire. Un filtre d'IA défaillant dans un centre d'exploitation portuaire est, selon ses propres termes, « une attaque interne perpétrée par des responsables de la sécurité incompétents ».

# CONCLUSIONS PRATIQUES POUR LES DÉCIDEURS DU SECTEUR MARITIME

Trois priorités méritent une attention particulière avant le prochain cycle budgétaire.

**Premièrement, une cartographie exhaustive de la surface d'attaque du port.** Les systèmes communautaires portuaires, les systèmes d'exploitation des terminaux, les VTS, les contrôleurs industriels, les flottes IoT, la 5G privée et les locataires du cloud hébergeant des charges de travail critiques doivent être inventoriés comme un périmètre continu, et non comme des projets cloisonnés. De nombreuses applications contiennent des composants issus d'anciennes bibliothèques open source, et l'externalisation vers le cloud a élargi le périmètre plus rapidement que les équipes de sécurité n'ont pu se développer. Savoir ce qui fonctionne, où et à qui cela est exposé n'est plus une option.

**Deuxièmement, des tests offensifs allant au-delà de la simple conformité.** Les audits traditionnels et les analyses automatisées ne permettront pas de mettre au jour les faiblesses enchaînées et inter-domaines qu'un véritable adversaire exploitera — celles qui relient un compartiment cloud mal configuré, une passerelle IoT oubliée et un workflow TOS pour former un incident capable de paralyser l'activité. Les ports ont besoin de spécialistes capables de maîtriser l'ensemble de cette pile et de penser comme un attaquant, en sondant les points les plus vulnérables sous pression — une créativité qui fait encore défaut aux modèles actuels.

**Troisièmement, la gouvernance de l'IA au sein de votre propre périmètre.** À mesure que les compagnies maritimes déploient des copilotes IA pour l'assistance à l'équipage, la maintenance prédictive ou le service client, chaque nouveau modèle devient une surface d'attaque et un canal potentiel de fuite de données.

La mer a toujours récompensé ceux qui savent anticiper les conditions météorologiques. Les attaques basées sur l'IA ne sont pas un scénario futuriste. Tout comme sur un navire, elles constituent le courant dans lequel nous naviguons déjà. La question est de savoir si l'équipage de votre passerelle dispose des instruments et des partenaires nécessaires pour maintenir le cap.

# 11.

# L'IA DEVIENT UN ACTEUR STRATÉGIQUE DANS LE CONFLIT DE L'INFORMATION

Contribution d'ATOS, analyse de la manipulation de l'information pilotée par l'IA et de la dimension de guerre cognitive des menaces hybride

**Les contenus deepfakes explosent depuis 2025. Le volume de fichiers deepfake est passé d'environ 500 000 contenus identifiés en 2023 à plus de 8 millions en 2025 selon EUvsDisinfo.**
**Les tentatives de fraude utilisant des contenus synthétiques ont progressé de 3 000 %.**

Depuis 2025, les États européens parlent désormais officiellement de « menace informationnelle ». La France a intégré cette dimension dans sa nouvelle doctrine. Ce changement est fondamental : il ne s'agit plus simplement de désinformation ou de fake news, mais d'un véritable champ de conflictualité stratégique visant à influencer les perceptions, les comportements et les décisions des individus, des entreprises et sociétés démocratiques.
Cette évolution repose sur une réalité simple : dans nos sociétés numériques, la donnée alimente tout. Les données nourrissent les informations. Les informations produisent du renseignement. Le renseignement oriente les décisions politiques, économiques, militaires ou sociétales ou des capitaines de navires.
Dès lors, si les données sont fausses, biaisées ou manipulées, toute la chaîne de décision peut être contaminée.
Plusieurs exemples récents montrent la puissance de ces menaces. Dans le détroit d'Ormuz, depuis le 28 février, la manipulation des signaux GPS, GNSS et AIS vise à produire une information fausse, un renseignement erroné pour provoquer un incident. Près d'un million d'incidents d'interférences de navigation satellitaire auraient été enregistrés, touchant environ 1 100 navires dès le premier jour de la crise de la guerre d'Iran selon le Mica Center. Les navires pouvaient apparaître sur de fausses positions : sur terre, dans des aéroports ou dans des zones incohérentes. Ces désinformations peuvent provoquer une erreur d'assurance, une mauvaise appréciation du risque, une décision de déroutement injustifiée ou, à l'inverse, une exposition dangereuse.
La donnée et l'information maritime sont devenues une ressource stratégique mais aussi une arme.

# UNE GUERRE COGNITIVE ALIMENTÉE PAR LES DONNÉES

Les conflits contemporains cherchent autant à détruire des infrastructures qu'à modifier les perceptions et comportements humains notamment avec l'utilisation de l'IA.
Un faux signal financier peut provoquer une panique boursière. Une vidéo truquée peut discréditer un dirigeant.
Une campagne algorithmique peut polariser une population.
Une manipulation de données avec seulement 250 documents peut produire des analyses erronées dans des systèmes d'IA.
Le phénomène s'est accéléré brutalement depuis 2025 avec une montée de nouvelle technique de manipulation.

# DES DÉTOURNEMENTS

Récemment, le FBI a alerté en avril 2026 sur la montée des vols de cargaisons. Le mode opératoire est typiquement informationnel et facilité par l'IA. Les attaquants usurpent l'identité de transporteurs ou de courtiers, publient de fausses annonces de fret, redirigent les cargaisons et manipulent les documents ou instructions logistiques ou clone des dirigeants. Les pertes estimées liées aux vols de cargaison aux États-Unis et au Canada ont atteint près de 725 millions de dollars en 2025, soit une hausse de 60 % par rapport à 2024. Ce n'est que le début.
Le problème dépasse désormais la simple désinformation.

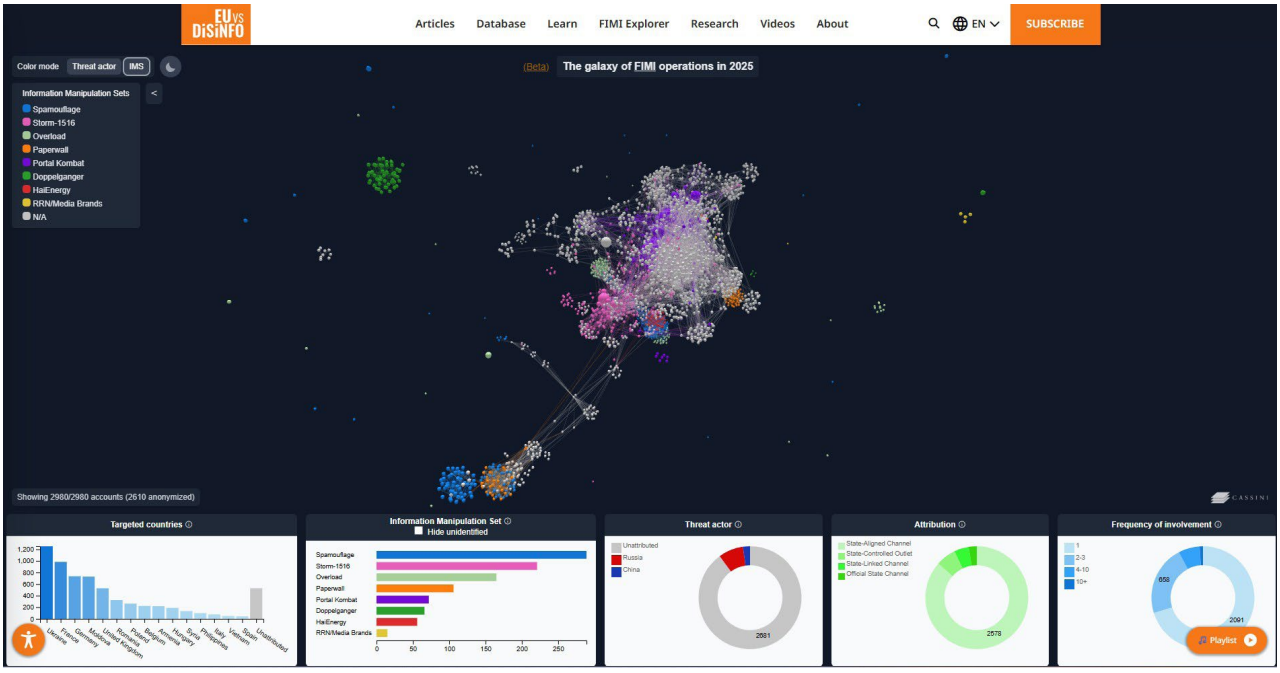
La guerre informationnelle et cognitive vise à influencer les émotions, les réflexes collectifs, la confiance et les comportements, voire les schémas neuronaux.
L'IA est le 4e acteur de conflit aux cotés des Etats, des organisations et des individus. Elle déclenche une rupture historique.
Elle devient un nouvel acteur autonome capable de produire, synthétiser, personnaliser et diffuser de l'information à une vitesse industrielle, de manière continue et capable de cibler toute personne selon ses centres d'intérêts ou angoisses.
Les IA génératives peuvent désormais :

- produire des milliers d'articles, vidéos ou messages crédibles ;
- cloner des voix humaines ;
- créer des avatars de décideurs ;
- automatiser des campagnes d'influence ;
- personnaliser les récits selon les profils psychologiques ou fonctions des décideurs ;
- couper des services numériques indispensables à un seul individu
- alimenter des agents conversationnels capables d'interagir massivement avec des citoyens ou individuellement.

# LA BATAILLE DE DEAMIN : PROTÉGER LES SYSTÈMES ET LES PRECEPTIONS

La nouvelle menace est informationnelle. Et l'IA en devient désormais l'un des principaux accélérateurs stratégiques mais aussi de défense.

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



# 12.

# RENFORCER LA RÉSILIENCE OPÉRATIONNELLE À L'ÈRE DES RISQUES HYBRIDES

Contribution de Alcyconie, gestion de crises cyber

# DE LA CYBER PROTECTION À LA RÉSILIENCE OPÉRATIONNELLE

Un incident cyber affectant un système communautaire portuaire, un système d'exploitation de terminal ou un service maritime critique peut désormais perturber les flux de fret dans plusieurs pays en l'espace de quelques heures. À mesure que les opérations maritimes deviennent de plus en plus interconnectées, le risque cybersécurité est passé d'une préoccupation purement technique à un défi opérationnel stratégique pour les ports, les compagnies maritimes, les autorités maritimes et les acteurs de la logistique.

S'appuyant sur l'expérience acquise lors d'exercices de crise cyber à grande échelle menés avec des organisations maritimes et portuaires à travers l'Europe, Alcyconie a observé un changement profond dans l'approche du secteur face au risque cyber. Alors que les organisations se concentraient initialement sur le renforcement des capacités techniques de protection et de détection, **les acteurs les plus expérimentés reconnaissent désormais que la résilience dépend tout autant de leur capacité à maintenir leurs opérations, à coordonner les parties prenantes et à prendre des décisions critiques sous pression.**

Le secteur maritime est confronté à des défis particuliers. Contrairement à de nombreux secteurs, il évolue au sein d'un écosystème fortement interconnecté où toute perturbation affectant une seule organisation peut se propager rapidement aux compagnies maritimes, aux exploitants de terminaux, aux prestataires logistiques, aux pilotes, aux autorités douanières et aux institutions publiques. Parallèlement, les infrastructures maritimes sont au cœur du commerce mondial et de la concurrence stratégique. Lors de plusieurs crises géopolitiques récentes, les ports, les routes maritimes et les écosystèmes logistiques sont devenus des cibles directes ou indirectes d'actions perturbatrices visant à exercer une pression économique, politique ou stratégique. En conséquence, la cyber-résilience n'est plus uniquement une question organisationnelle. Elle repose de plus en plus sur la capacité collective des communautés maritimes à anticiper, à résister et à réagir efficacement aux crises pouvant combiner cyberattaques, perturbations opérationnelles, répercussions sur la chaîne d'approvisionnement et dynamiques géopolitiques.

# RENFORCER LA GOUVERNANCE ET L'ORGANISATION EN CAS DE CRISE

La mise en œuvre de la directive NIS2, conjuguée aux préoccupations croissantes concernant la continuité des activités, accélère l'évolution de la gouvernance des crises cyber dans l'ensemble du secteur maritime.
Au sein des organisations accompagnées par Alcyconie, plusieurs priorités communes se dégagent :

- Mettre en place des processus clairs d'alerte, d'escalade et de prise de décision allant au-delà des équipes techniques ;
- Intégrer les fournisseurs, sous-traitants et partenaires opérationnels essentiels dans les dispositifs de gestion de crise ;
- Renforcer les plans de continuité d'activité et de reprise pour les services maritimes essentiels et les opérations logistiques ;
- Améliorer la coordination entre la direction générale, les équipes opérationnelles et les spécialistes de la cybersécurité.

Ces évolutions reflètent une prise de conscience plus large selon laquelle les incidents cyber ne peuvent plus être considérés uniquement comme des événements informatiques. Dans le secteur maritime, les perturbations peuvent affecter l'exploitation des navires, la gestion des cargaisons, les chaînes logistiques, les communications ou

les services publics, ce qui nécessite des réponses coordonnées impliquant plusieurs fonctions et organisations.
En conséquence, les exercices de simulation de crises cyber sont devenus un élément central des programmes de résilience, permettant aux organisations de valider leurs structures de gouvernance et d'identifier les faiblesses potentielles avant qu'un incident réel ne se produise.

## SE PRÉPARER AUX CRISES DE DEMAIN

Si les ransomwares, les attaques par déni de service et les compromissions de systèmes restent des préoccupations majeures, les organisations maritimes reconnaissent de plus en plus que les crises futures sont susceptibles de combiner des dimensions cybernétiques, opérationnelles, informationnelles et géopolitiques. La nature des exercices a donc considérablement évolué.

Pour les organisations qui entament leur parcours vers la résilience, les exercices visent principalement à valider les cadres de gestion de crise, à clarifier les responsabilités et à améliorer la coordination entre les parties prenantes techniques, opérationnelles et dirigeantes.

Pour les organisations plus matures, les objectifs sont plus larges. Les exercices impliquent de plus en plus les environnements technologiques opérationnels, les unités opérationnelles, les comités de direction et les partenaires externes. L'accent n'est plus mis sur la réponse technique, mais sur la prise de décision stratégique, la continuité des opérations et la coordination des parties prenantes dans des conditions d'incertitude. Cette évolution reflète le changement de paysage des menaces.

Pour un secteur qui se trouve en première ligne du commerce mondial et des tensions géopolitiques, la prospective stratégique n'est plus une option. Les organisations maritimes doivent sans cesse regarder au-delà des menaces actuelles et développer leur capacité à anticiper les nouvelles formes de perturbations. Qu'elles soient liées à l'innovation technologique, à l'instabilité géopolitique, aux dépendances au sein de la chaîne d'approvisionnement ou à des opérations d'influence hybrides, les crises futures ne ressembleront probablement pas à celles du passé. Renforcer la résilience nécessite donc non seulement d'être prêt, mais aussi de cultiver une culture d'anticipation et d'adaptation continue.

Dans ce contexte, les exercices de simulation de crises cyber sont de plus en plus utilisés comme outil de prospective stratégique. Au-delà de la validation des procédures existantes, ils permettent aux organisations d'explorer des scénarios futurs plausibles, de remettre en question leurs hypothèses et de préparer les décideurs à des crises qui ne se sont pas encore produites, mais qui pourraient avoir un impact significatif sur les opérations maritimes et la continuité des activités.

Les tensions géopolitiques croissantes, les interdépendances au sein des chaînes d'approvisionnement, la dépendance vis-à-vis de tiers essentiels et l'émergence de menaces hybrides créent des scénarios dont les conséquences s'étendent bien au-delà des systèmes d'information. Les organisations maritimes sont de plus en plus exposées à des situations où de multiples perturbations se produisent simultanément : compromission d'un fournisseur stratégique, indisponibilité prolongée des systèmes opérationnels, perturbation des chaînes logistiques, campagnes de désinformation ciblant les activités portuaires, ou encore actions coordonnées visant à saper la confiance et les performances opérationnelles.

Au cours de l'année écoulée, Alcyconie a notamment mis au point des simulations de crise avancées pour de grands acteurs internationaux du secteur maritime, notamment des scénarios combinant cyberattaques, perturbations opérationnelles et opérations d'influence. Ces exercices ne visent pas à prédire la prochaine crise, mais à confronter les organisations à des situations plausibles qui remettent en question leurs hypothèses existantes et testent leur capacité à s'adapter sous pression.

# ENSEIGNEMENTS TIRÉS DES EXERCICES DE CRISE MARITIME

Plusieurs observations récurrentes se dégagent des exercices menés avec des organisations maritimes et portuaires :

- Les répercussions opérationnelles sont souvent sous-estimées par rapport aux répercussions techniques ;
- La dépendance vis-à-vis des fournisseurs et des prestataires de services externes constitue fréquemment une vulnérabilité critique ;
- La prise de décision au niveau de la direction joue un rôle décisif dans la limitation des conséquences d'un incident ;
- La communication avec les clients, les partenaires, les autorités et les médias devient rapidement un enjeu stratégique ;
- La coordination au sein de l'écosystème maritime s'avère souvent plus difficile que la mise en œuvre des mesures correctives techniques elles-mêmes.

Ces conclusions illustrent une transformation plus large en matière de préparation aux cybermenaces. Les organisations ne cherchent plus seulement à améliorer leur capacité à détecter les cyberattaques et à y répondre. Elles s'efforcent de plus en plus de renforcer leur capacité à maintenir le contrôle opérationnel, à préserver les services essentiels et à prendre des décisions éclairées malgré l'incertitude et le manque d'informations.

# PERSPECTIVES D'AVENIR

Le secteur maritime se trouve au carrefour du commerce mondial, des infrastructures stratégiques et de la concurrence géopolitique. Alors que les cybermenaces ne cessent d'évoluer, la résilience ne peut plus être mesurée uniquement à l'aune de la solidité des défenses techniques.

Les organisations qui se montreront les plus résilientes seront celles capables de maintenir la continuité opérationnelle, de coordonner efficacement leurs actions au sein d'écosystèmes complexes et de prendre des décisions critiques sous pression.

Dans un contexte où les risques de cybersécurité, opérationnels, informationnels et géopolitiques convergent de plus en plus, la résilience est devenue une capacité collective. Pour les acteurs du secteur maritime, se préparer à cette réalité par le biais d'exercices de crise réalistes et ambitieux n'est plus une option : c'est une nécessité stratégique.

# CONTRIBUTEURS DE CETTE ÉDITION

## FRANCE CYBER MARITIME REMERCIE LES ORGANISATIONS SUIVANTES POUR LEUR CONTRIBUTION.

**Alcyconie** – gestion des crises cyber, certifié PACS par l'ANSSI.

**ATOS** – analyse de la manipulation de l'information pilotée par l'IA et de la dimension de guerre cognitive des menaces hybrides.

**BZHunt** – cybersécurité offensive, tests d'intrusion et exercices de simulation d'attaques (« red teaming »), en Bretagne, France.

**DIATEAM** – Hybrid Cyber Range et formation à la cybersécurité maritime.
• contact@diateam.net

**FMES (Fondation pour la Maîtrise des Enjeux Stratégiques)** – de réflexion français spécialisé dans la recherche stratégique.

**GLIMPS** – analyse approfondie de fichiers et caractérisation des logiciels malveillants grâce à l'IA, reposant sur une technologie de Deep Learning souveraine.

**Marlink** – connectivité maritime et renseignements sur les cybermenaces.
• cti@marlink.com

**Orange Cyberdefense** – filiale du groupe Orange spécialisée dans la cybersécurité.

**Semsoft (LESTR)** – fusion de données et IA pour la détection des risques liés au commerce maritime.
• business@lestr.app

**XRATOR** – renseignements et analyse des menaces de cybersécurité.

# 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

AVEC LE SOUTIEN DE

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