LA GESTION DES CYBER-RISQUES MARITIMES
Décryptage réglementaire

CONTEXTE ET ENJEUX

Le milieu maritime est confronté à de nouveaux risques notamment ceux liés à l'utilisation d'outils informatiques à bord. Les **atteintes directes ou indirectes contre les systèmes de traitement automatisé de données** des navires, des plateformes pétrolières ou des ports font l'objet d'une préoccupation grandissante de la part du secteur maritime.

Depuis quelques années le secteur est en effet la cible de cyberattaques, comme le port d'Anvers en 2011 ou l'armateur danois A.P. Møller-Mærsk en 2017. Les menaces sont diverses et ont un **impact opérationnel conséquent**. Elles représentent des enjeux pour la sûreté et la sécurité des personnes et des biens, en mer et au port.

RÉGLEMENTATION

Au niveau international

Actuellement il n'existe **aucune réglementation internationale obligatoire** applicable aux questions de cybersécurité intéressant le secteur maritime. Pour autant, des outils développés dans l'enceinte de l'Organisation Maritime Internationale (OMI) visent à répondre à ces enjeux cruciaux.

Le **Code ISPS**[1], instrument réglementaire de référence en matière de sûreté maritime, prévoit ainsi dans sa partie facultative que *« l'évaluation de la sûreté du navire devrait porter sur les [...] systèmes de radio et télécommunications, y compris les systèmes et réseaux informatiques »*. Le **Code ISM**[2]**,** par ses exigences génériques, englobe également sans les citer les cyber-risques émergents. Il oblige chaque compagnie à proposer **des pratiques d'exploitation et un environnement de travail sans danger**, à évaluer tous les risques identifiés pour les navires, leur personnel et l'environnement, et à établir des mesures de précaution appropriées, l'objectif étant d'améliorer constamment les compétences du personnel à terre et à bord des navires.

Par ailleurs, consciente des risques encourus, l'OMI a publié en 2017 des **directives sur la gestion des cyber-risques maritimes**[3] qui fournissent des recommandations et visent à protéger les transports maritimes contre les cyber-menaces.

[1] ISPS pour International Ship and Port Facility Security signifie « Code international pour la sûreté des navires et des installations portuaires ». Le Code ISPS est entré en vigueur le 1er juillet 2004.
[2] ISM pour International Safety Management signifie « Code international de gestion de la sécurité ». Le code ISM est entré en vigueur le 1er juillet 2002.
[3] Circulaire MSC.1-FAL.1/Circ.3.

De plus, le Comité de la Sécurité Maritime de l'OMI (MSC) a adopté courant 2017, une résolution relative à la gestion des cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité[4]. Dans un souci d'efficacité et d'adaptabilité, l'OMI envisage, dans cette résolution, la question cyber seulement à travers le code ISM. Les travaux du MSC se poursuivent actuellement pour perfectionner les dispositions produites en 2017. La délégation des États-Unis et plusieurs organisations représentatives du shipping ont ainsi pu soumettre des **propositions en faveur d'une application uniforme des directives** sur la gestion des cyber-risques maritimes et d'une harmonisation des exigences du code ISM et du code ISPS sur cette thématique[5].

Les travaux de l'OMI sont complétés par ceux des associations maritimes internationales comme l'*International Chamber of Shipping* (ICS) qui a publié des recommandations en matière de cybersécurité. De son côté, le *Baltic and International Maritime Council* (BIMCO) a développé une série de clauses types liées à la cybersécurité, à intégrer aux chartes-parties[6].

Au niveau européen

La **directive NIS**[7] (UE) n°2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 prévoit la mise en œuvre de mesures destinées à assurer un niveau élevé et commun de sécurité des réseaux et des systèmes d'information au sein de l'Union Européenne**.**

Cette directive et les moyens à déployer soulignent la criticité des réseaux et des systèmes d'information ainsi que la nécessité d'apporter une réponse unifiée à l'échelle de l'Europe, aux risques pesant sur les entreprises et leur niveau de cybersécurité, en définissant des obligations à destination des États et des opérateurs.

En France, cette directive a été transposée dès 2018. Elle identifie notamment les **Opérateurs de Services Essentiels** dits « OSE », qui fournissent un service dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société. Les compagnies de transport maritime et les gestionnaires de ports sont soumis à ces dispositions. Pour ces opérateurs, des **mesures techniques et organisationnelles** doivent être adoptées afin de les protéger contre les cyber-risques.

Il existe une collaboration soutenue au sein de l'UE entre l'industrie, les États membres et l'Agence Européenne chargée de la Sécurité des Réseaux et de l'Information (ENISA) et un **point de contact unique a été créé à cette fin**. Une ou des **équipes d'intervention en cas d'urgence informatique** doivent assurer une gestion des incidents et des risques.

[4] Résolution MSC.428(98).
[5] Voir les travaux du Comité de la sécurité maritime lors de sa 101ème session.
[6] Une charte-partie matérialise un contrat d'affrètement par lequel le fréteur met un navire à disposition de l'affréteur.
[7] NIS pour Network and Information System Security.

Au niveau national

La réglementation nationale intègre les exigences spécifiques du code ISPS dans la **division 130** annexée à l'arrêté de 1987 relatif à la sécurité des navires (article 130-39). Par ces dispositions, la France impose aux armateurs d'évaluer le risque cyber et de mettre en place de nouvelles mesures, notamment dans le **plan de sûreté du navire**. Ce document confidentiel et obligatoire définit ainsi les procédures à appliquer pour chaque risque identifié.

Cette évaluation doit statuer au moins sur :

- la cartographie logicielle et matérielle du navire ;
- la définition des éléments sensibles du navire ;
- la gestion des vulnérabilités des systèmes.

L'**évaluation** doit formaliser les mesures adoptées par la compagnie en termes de protection des systèmes de communication et d'information au niveau du plan de sûreté du navire. Ces mesures portent sur le résultat de l'évaluation, le seuil de probabilité d'accident, les systèmes clés du navire, les conclusions d'ordres politique et technique relatives à la cybersécurité du navire.

Des dispositions avaient déjà été adoptées de 2013 à 2016, précédent le dispositif NIS européen et les directives OMI. Celles-ci sont destinées à protéger les « **Opérateurs d'Importance Vitale** (OIV)[8] » (loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 -art. 22) et notamment ceux du sous-secteur « Transports maritime et fluvial » (arrêté du 11 août 2016).

Par ailleurs, l'**Agence Nationale de la Sécurité des Systèmes d'Information** (ANSSI)[9] a publié trois guides pour la sensibilisation des compagnies et des marins disponibles gratuitement sur le site du ministère de la transition énergétique et solidaire :

- « *Cybersécurité : Évaluer et protéger le navire* » (2016) ;
- « *Guide des bonnes pratiques de sécurité informatique à bord des navires* » (2016) ;
- « *Cybersécurité : Renforcer la protection des systèmes industriels du navire* » (2017).

Enfin, la **formation initiale** des étudiants à l'École Nationale Supérieure Maritime (ENSM) intègre depuis 2017 deux jours de sensibilisation destinés à l'étude des risques et des évènements majeurs liés au cyber, à la prévention et à la diffusion des bons gestes. En partenariat avec plusieurs autres organismes de formation, des réflexions sont conduites sur la création d'un mastère spécialisé en matière de cybersécurité des systèmes maritimes et portuaires. Une **plateforme de simulation** est également à l'étude pour éprouver la marétique[10] et le facteur humain face aux cyber-risques maritime

[8] Un opérateur d'importance vitale (OIV) est, en France, une organisation identifiée par l'État comme ayant des activités indispensables ou dangereuses pour la population.
[9] Éclairage de Thibaut Marrel, spécialiste de la cybersécurité à l'ANSSI, page 38 du Rapport annuel 2018/2019 d'Armateurs de France.
[10] L'ensemble des technologies liées au domaine maritime.