ORGANISATION MARITIME INTERNATIONALE

F

4 ALBERT EMBANKMENT
LONDRES SE1 7SR
Téléphone : +44 (0)20 7735 7611 Télécopieur : +44 (0)20 7587 3210

MSC-FAL.1/Circ.3/Rev.2
7 juin 2022

DIRECTIVES SUR LA GESTION DES CYBER-RISQUES MARITIMES

1 Le Comité de la simplification des formalités, à sa quarante et unième session (4-7 avril 2017) et le Comité de la sécurité maritime, à sa quatre-vingt-dix-huitième session (7-16 juin 2017), considérant qu'il était urgent de faire mieux connaître les menaces et vulnérabilités liées aux cyber-risques, ont approuvé les Directives sur la gestion des cyber-risques maritimes, dont le texte figure en annexe à la présente circulaire.

2 Les Directives fournissent des recommandations de haut niveau sur la gestion des cyber-risques maritimes visant à protéger les transports maritimes contre les cybermenaces et vulnérabilités actuelles et émergentes. Elles comprennent également les éléments fonctionnels sur lesquels repose une gestion efficace des cyber-risques.

3 Le Comité de la sécurité maritime, à sa cent quatrième session (4-8 octobre 2021), et le Comité de la simplification, à sa quarante-sixième session (9-13 mai 2022), ont approuvé une mise à jour des orientations et normes complémentaires qui figurent au paragraphe 4.2 des Directives.

4 Les Gouvernements Membres sont invités à porter le contenu de la présente circulaire à l'attention de toutes les parties prenantes intéressées.

5 La présente circulaire et tout amendement qui lui serait apporté annulent et remplacent la circulaire MSC.1/Circ.1526 dans laquelle figuraient les Directives intérimaires.

***

ANNEXE

DIRECTIVES SUR LA GESTION DES CYBER-RISQUES MARITIMES

1 INTRODUCTION

1.1 Les présentes Directives ont pour objet de fournir des recommandations de haut niveau sur la gestion des cyber-risques maritimes. Aux fins des présentes Directives, le cyber-risque maritime désigne une quantification de la mesure dans laquelle une ressource technologique est menacée par une circonstance ou un événement susceptible de se produire qui pourrait entraîner des défaillances opérationnelles et des lacunes en matière de sécurité ou de sûreté dues à la corruption, à la perte ou à l'altération des informations ou des systèmes.

1.2 Les parties prenantes devraient prendre les mesures qui s'imposent afin de protéger les transports maritimes contre les menaces et vulnérabilités actuelles et émergentes relatives à la numérisation, à l'intégration et à l'automatisation des processus et systèmes des transports maritimes.

1.3 Pour obtenir des renseignements précis et des orientations au sujet de la mise au point et de l'exécution de processus spécifiques de gestion des risques, les utilisateurs des présentes Directives devraient consulter les prescriptions spécifiques des Gouvernements Membres et des Administrations de l'État du pavillon, les normes internationales et les normes du secteur pertinentes, ainsi que les meilleurs pratiques en la matière.

1.4 La gestion des risques est essentielle pour garantir la sécurité et la sûreté des opérations maritimes. Jusqu'à présent, la gestion des risques portait sur les opérations effectuées dans le domaine physique, mais le recours accru à la numérisation, à l'intégration, à l'automatisation et aux systèmes en réseau a renforcé le besoin de prévoir une gestion des cyber-risques dans le secteur des transports maritimes.

1.5 Ayant pour objet de contribuer à la sécurité et à la sûreté des transports maritimes, dont l'exploitation est résiliente face aux cyber-risques, les présentes Directives fournissent des recommandations qui peuvent être incorporées dans les processus de gestion des risques existants. À cet égard, les Directives complètent les pratiques en matière de gestion de la sécurité et de la sûreté établies par l'Organisation.

2 GÉNÉRALITÉS

2.1 Rappel des faits

2.1.1 Les cybertechnologies sont devenues essentielles pour exploiter et gérer de nombreux systèmes qui jouent un rôle déterminant dans la sécurité et la sûreté des transports maritimes et dans la protection du milieu marin. Dans certains cas, ces systèmes doivent satisfaire aux normes internationales et aux prescriptions de l'Administration de l'État du pavillon. Toutefois, les vulnérabilités créées par l'accès à ces systèmes, leur interconnexion ou leur mise en réseau peuvent engendrer des cyber-risques qu'il faudrait traiter. Parmi les systèmes vulnérables pourraient notamment figurer les éléments ci-après :

- systèmes de passerelle;
- systèmes de manutention et de gestion de la cargaison;
- systèmes de gestion de la propulsion et des machines et systèmes de contrôle de l'énergie;

- systèmes de contrôle de l'accès;
- systèmes de service aux passagers et de gestion des passagers;
- réseaux publics destinés aux passagers;
- systèmes administratifs et systèmes récréatifs des membres d'équipage; et
- systèmes de communication.

2.1.2 Il faudrait tenir compte de la différence qui existe entre les systèmes des technologies de l'information et les systèmes des technologies opérationnelles. Les premiers peuvent être considérés comme axés sur l'utilisation des données en tant qu'informations et les seconds comme axés sur l'utilisation des données aux fins de contrôler ou de surveiller des processus physiques. En outre, il faudrait tenir compte également de la protection de l'information et de l'échange de données dans le cadre de ces systèmes.

2.1.3 Si ces technologies et systèmes représentent d'importants gains d'efficacité pour le secteur maritime, ils présentent également des risques pour les systèmes et processus essentiels associés à l'exploitation des systèmes qui font partie intégrante des transports maritimes. Ces risques peuvent découler de vulnérabilités dues à une exploitation, une intégration, une maintenance et une conception inadéquates des cybersystèmes, ainsi que de cybermenaces intentionnelles et non intentionnelles.

2.1.4 Les menaces se présentent sous la forme d'attaques malveillantes (par exemple piratage ou introduction de logiciels malveillants) ou sont la conséquence inattendue d'activités anodines (par exemple maintenance des logiciels ou gestion des droits d'utilisateurs). D'une manière générale, ces activités mettent au jour des vulnérabilités (par exemple le caractère obsolète des logiciels ou l'inefficacité des pare-feu) ou tirent parti d'une vulnérabilité des technologies opérationnelles ou des technologies de l'information. Pour que la gestion des cyber-risques soit efficace, il faudrait tenir compte de ces deux types de menaces.

2.1.5 Les vulnérabilités peuvent découler d'insuffisances en matière de conception, d'intégration et/ou de maintenance des systèmes, ainsi que de manquements à la cyberdiscipline. En général, lorsque des vulnérabilités des technologies opérationnelles et/ou des technologies de l'information sont révélées ou exploitées, soit directement (par exemple, des mots de passe faciles à deviner entraînant un accès non autorisé) soit indirectement (par exemple, absence de cloisonnement des réseaux), elles peuvent avoir une incidence sur la sûreté et sur la confidentialité, l'intégrité et la disponibilité des informations. Elles peuvent également avoir une incidence sur la sécurité, en particulier lorsque des systèmes essentiels (par exemple les systèmes de navigation à la passerelle ou les systèmes de propulsion principaux) sont compromis.

2.1.6 Une gestion efficace des cyber-risques devrait également comprendre les incidences, du point de vue de la sécurité et de la sûreté, qui résultent de la mise au jour ou de l'exploitation de vulnérabilités des systèmes des technologies de l'information. Ces vulnérabilités pourraient découler d'une connexion inappropriée à des systèmes des technologies opérationnelles ou d'erreurs de procédure commises par le personnel chargé de l'exploitation ou par des tiers, qui peuvent porter atteinte à ces systèmes (par exemple l'utilisation inappropriée de supports amovibles comme une clé USB).

2.1.7 On trouvera de plus amples renseignements sur les vulnérabilités et les menaces dans les orientations et normes supplémentaires mentionnées dans la section 4.

2.1.8 Du fait de l'évolution rapide de ces technologies et de ces menaces, il est difficile de traiter ces risques uniquement par le biais de normes techniques. C'est pourquoi il est recommandé dans les présentes Directives d'adopter une approche de la gestion des cyber-risques qui soit résiliente et qui évolue dans le prolongement naturel des pratiques existantes en matière de gestion de la sécurité et de la sûreté.

2.1.9 Lorsque l'on examine les sources potentielles de menaces et de vulnérabilités, ainsi que les stratégies connexes d'atténuation des risques, il faudrait également prendre en considération un certain nombre d'options de contrôle possibles aux fins de la gestion des cyber-risques, parmi lesquelles le contrôle de gestion, le contrôle opérationnel ou procédural et le contrôle technique.

2.2 Champ d'application

2.2.1 Les présentes Directives sont avant tout destinées à toutes les organisations du secteur maritime et ont pour objet de promouvoir l'adoption de pratiques de gestion de la sécurité et de la sûreté dans le cyberdomaine.

2.2.2 Compte tenu des caractéristiques propres à chacune des organisations du secteur maritime, les présentes Directives sont rédigées en termes généraux afin d'être largement appliquées. Les navires équipés de cybersystèmes limités jugeront peut-être suffisante la simple application des présentes Directives mais les navires équipés de cybersystèmes complexes auront peut-être besoin d'un niveau de protection accru et devraient chercher à obtenir des ressources supplémentaires auprès de partenaires fiables du secteur et des pouvoirs publics.

2.2.3 Les présentes Directives ont valeur de recommandation.

3 ÉLÉMENTS DE LA GESTION DES CYBER-RISQUES

3.1 Aux fins des présentes Directives, la *gestion des cyber-risques* désigne le processus consistant à identifier, analyser, évaluer et communiquer des cyber-risques et à les accepter, les éviter, les transférer ou les atténuer en les ramenant à un niveau acceptable compte tenu des coûts et des avantages des mesures prises pour les parties prenantes.

3.2 La gestion des cyber-risques maritimes a pour objet de contribuer à la sécurité et la sûreté des transports maritimes, dont l'exploitation est résiliente aux cyber-risques.

3.3 Pour être efficace, la gestion des cyber-risques devrait commencer au niveau de la direction. Les cadres supérieurs devraient créer, à tous les niveaux d'une organisation, une culture de sensibilisation aux cyber-risques et s'assurer que les mesures de gestion relèvent d'une démarche holistique et souple qui soit appliquée en permanence et qui fasse l'objet d'une évaluation constante au moyen de mécanismes efficaces de retour d'information.

3.4 L'une des approches acceptées pour y parvenir consiste à évaluer et à comparer de manière approfondie les positions actuelle et souhaitée d'une organisation en matière de gestion des cyber-risques. Une telle comparaison peut révéler des lacunes qui peuvent être comblées dans le cadre d'un plan de gestion des cyber-risques classés par ordre de priorité, en vue d'atteindre les objectifs de gestion des risques. Cette approche fondée sur les risques permettra à une organisation d'utiliser ses ressources de la manière la plus efficace.

3.5 Les présentes Directives exposent les éléments fonctionnels sur lesquels repose la gestion efficace des cyber-risques. Ces éléments fonctionnels ne suivent pas un ordre défini : ils devraient tous être simultanés et continus dans la pratique et être intégrés comme il convient dans un cadre de gestion des risques :

1. Identifier : définir les fonctions et responsabilités du personnel en matière de gestion des cyber-risques et recenser les systèmes, les biens, les données et les moyens qui, lorsqu'ils sont perturbés, présentent des risques pour les opérations du navire.

2. Protéger : mettre en œuvre des processus et mesures de maîtrise des risques pour éviter tout cyberévénement et garantir la continuité des opérations des transports maritimes.

3. Détecter : élaborer et mettre en œuvre les activités nécessaires pour détecter rapidement un cyberévénement.

4. Intervenir : élaborer et mettre en œuvre des activités et des plans propres à assurer la résilience et le rétablissement des systèmes nécessaires aux opérations ou services maritimes qui ont été compromis par un cyberévénement.

5. Récupérer : recenser les mesures à prendre pour sauvegarder et rétablir les cybersystèmes nécessaires aux opérations des transports maritimes qui ont été compromis par un cyberévénement.

3.6 Ces éléments fonctionnels comprennent les activités et résultats souhaités d'une gestion efficace des cyber-risques dans l'ensemble des systèmes essentiels pour les opérations du secteur maritime et l'échange d'informations et constituent un processus continu comportant des mécanismes efficaces de retour d'information.

3.7 La gestion efficace des cyber-risques devrait assurer un degré approprié de connaissance des cyber-risques à tous les niveaux d'une organisation. Le degré de sensibilisation et de préparation aux risques devrait correspondre aux rôles et aux responsabilités à assumer dans le système de gestion des cyber-risques.

4 MEILLEURES PRATIQUES POUR LA MISE EN ŒUVRE DE LA GESTION DES CYBER-RISQUES

4.1 L'approche de la gestion des cyber-risques qui est décrite dans les présentes Directives jette les bases pour mieux comprendre et gérer les cyber-risques, ce qui permettra de définir une approche en matière de gestion des risques qui réponde aux cybermenaces et aux vulnérabilités. Pour obtenir des orientations détaillées au sujet de la gestion des cyber-risques, les utilisateurs des présentes Directives devraient également consulter les prescriptions des Gouvernements Membres et des Administrations des États du pavillon, ainsi que les normes internationales et les normes du secteur pertinentes, de même que les meilleures pratiques en la matière.

4.2 Les orientations et les normes supplémentaires peuvent inclure, sans toutefois s'y limiter, les documents suivants :*

.1 les Directives sur la cybersécurité à bord des navires, produites et appuyées par BIMCO, l'ICS, INTERCARGO, INTERTANKO, InterManager, l'OCIMF, l'IUMI, SYBAss et le WSC;

.2 la version récapitulative de la Recommandation de l'IACS sur la cyber-résilience (Recommandation 166);

.3 la norme ISO/CEI 27001 sur les Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, publiée conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI); et

.4 le Cadre pour l'amélioration de la cybersécurité dans les infrastructures essentielles (cadre NIST) du National Institute of Standards and Technology des États-Unis.

.5 Directives de l'IAPH sur la cybersécurité dans les ports et les installations portuaires.

4.3 Il y a lieu de se reporter à la version la plus récente de toutes directives ou normes utilisées.

---

* Les orientations et les normes supplémentaires sont fournies à titre indicatif pour que les utilisateurs des présentes Directives puissent obtenir de plus amples détails mais il ne s'agit pas d'une liste exhaustive. Elles n'ont pas été publiées par l'Organisation et leur utilisation est laissée à l'appréciation de chaque utilisateur.