Cyber sécurité
Note d'information

REGLEMENTATION :

Au niveau international :

Il n'existe actuellement pas de règlementation internationale obligatoire qui traite directement de ce sujet. Par contre, on retrouve dans certains règlements internationaux obligatoires des dispositions qui permettent de prendre en compte le risque cyber.
On peut citer les codes ISM et ISPS. Ils ne traitent pas spécifiquement de ce sujet, mais qui permettent de prendre en compte le risque cyber via le management de la sécurité à bord du navire et la sûreté du navire et des ports. Par exemple :

- Code ISPS A9.4.2 : « appliquer les mesures de protections physiques des systèmes d'information du navire »
- Code ISM : chapitre 1« rédiger une politique compagnie sur les systèmes d'information du navire »
- Code ISM Chapitre 7 : « appliquer un contrôle des échanges des systèmes d'information du navire »

Par ailleurs, consciente des risques encourus, l'OMI a rédigé le document « *directives intérimaires sur la gestion des cyber-risques maritimes* ». (MSC.1 Circ.1526). C'est une première pierre qui marque le début de travaux importants au niveau international et l'évolution vers une règlementation internationale obligatoire.
En Juin 2017, lors du MSC 98 la France et des Etats Unis ont soumis un document qui propose d'intégrer au niveau du système de gestion de sécurisé du navire une évaluation du cyber risque au plus tard à la première vérification annuelle du document de conformité de la compagnie après le 1er janvier 2021. Cette proposition (résolution MSC.428(98)) est en cours de validation.

D'autre part, la seconde émission du guide BIMCO « the guidelines on cyber security onboard ships » a été publié. Cette nouvelle version inclue la création d'un chapitre relatif à la gestion de l'assurance en cas de cyber attaque, la gestion concernant la séparation des réseaux et la gestion concernant la communication entre le navire et l'interface terrestre. Elle intègre également une nouvelle rédaction du chapitre relatif à la gestion du plan d'urgence,

Au niveau européen :

La directive 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Européenne (« directive NIS ») prévoit la mise en place par les Etats membres de stratégies pour la sûreté des réseaux et de l'information, et organise la coopération entre Etats membres.

Champ d'application :

La directive s'applique aux « opérateurs de services essentiels ». Ce sont les opérateurs de type listés à l'annexe II, qui remplissent les conditions suivantes :

- Ils fournissent un service essentiel pour le maintien d'activités sociales et/ou économiques,
- La fourniture de ce service dépend des réseaux et des systèmes d'information,
- Tout incident survenant sur les réseaux et systèmes d'information nuit à la fourniture du service. Ce critère est évalué en fonction du nombre d'utilisateurs, de la dépendance d'autres secteurs au service, de l'impact des incidents sur les activités socio-économiques et/ou la sécurité publique, la part de marché de l'opérateur, l'aire géographique affectée, et la possibilité de maintenir un service minimal ou de mettre en place des alternatives.

L'annexe II.2.c fait référence :

- Aux compagnies de transports maritime et fluvial de passagers et de fret, tels que définies à l'annexe I du règlement 725/2004[1], à l'exclusion des navires. En d'autres termes, seuls les installations à terre (bureaux) sont concernées. Cette exclusion fait suite à l'intervention de l'industrie[2] ;
- Aux autorités gestionnaires des ports et aux opérateurs de terminaux ;
- Aux opérateurs de services de gestion du trafic.

Toutes les compagnies appliquant l'ISM ne seront pas forcément désignées comme « opérateurs de services essentiels » car il faut également prendre en compte les autres critères définis dans le champ d'application.

Dispositions applicables aux Etats :

- Etablir la **liste** de ces opérateurs disposant d'un établissement sur leur territoire, puis la mettre à jour tous les deux ans ;
- Mettre en place une **stratégie pour la sécurité des réseaux et de l'information**[3],
- Désigner une ou plusieurs **autorités compétentes** (contrôle de la mise en œuvre de la directive), un **point de contact unique** (coopération entre Etats), et une ou des **équipes**

[1] Cette annexe reprend les dispositions du code ISPS :
7. Compagnie désigne une compagnie telle que définie à la règle IX/1. « *Company* means the owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for the operation of the ship from the owner of the ship and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the International Safety Management Code." Nous interprétons ce renvoi à SOLAS comme signifiant que l'ensemble des compagnies maritimes, y compris 'de service' sont concernées.

[2] On notera que les opérateurs de services de transport aériens et ferroviaires sont également listés à l'annexe II, mais pas les opérateurs routiers.

[3] Enonçant :

- Les objectifs de la stratégie ;
- Les modalités de gouvernance applicables, et la liste des acteurs impliqués dans l'élaboration de la stratégie ;
- Les mesures de préparation, de réponse et de remise en état, y compris la coopération avec le secteur privé ;
- Les mesures de sensibilisation et de formation ;
- Les actions de R&D liées ;
- L'évaluation des risques ;

d'intervention en cas d'urgence informatique (gestion des incidents et des risques)**.** Ces fonctions peuvent être exercées par une seule entité.

La Commission assure le secrétariat d'un **groupe de coopération** entre les Etats membres. Un **réseau réunissant les équipes d'intervention** est également créé.

Dispositions applicables aux opérateurs :

Les opérateurs de services essentiels **prennent les mesures techniques et organisationnelles** nécessaires pour gérer les risques de manière appropriée. Ils prennent notamment les mesures appropriées pour prévenir et réduire les incidents, afin d'assurer la continuité de leurs services. Tout incident ayant un impact significatif sur la continuité de service est **notifié** à l'autorité compétente ou à l'équipe d'intervention. L'autorité compétente peut décider d'informer le public d'un incident particulier si la situation le justifie.

Les Etats encouragent l'usage de standards et/ou spécifications européens et internationaux, sans les imposer.

Un considérant dispose que les Etats membres devront tenir compte des codes et lignes directrices, actuels et à venir, en particulier ceux développés par l'OMI, lorsqu'ils identifient les opérateurs maritimes, et ce à des fins d'harmonisation. Le considérant suivant prévoit que les dispositions maritimes spécifiques prévoyant le reporting d'incidents sûreté, prévalent sur la directive NIS s'ils sont au moins équivalents ; il est reflété à l'article 1.7, qui n'est pas spécifique au maritime.

Dispositions nationales :

La réglementation nationale qui reprend le code ISPS est la Division 130 A130-39.

La France a imposé au niveau de sa réglementation nationale, la nécessité d'évaluer les dispositions relatives à la cyber sécurité. Les armateurs doivent évaluer ce risque et mettre en place de nouvelles mesures. Cela se reflète dans le document « plan de sécurité du navire » qui est un document confidentiel et obligatoire, et qui définit les procédures à appliquer en fonction de chaque risque identifié.

Cette évaluation doit statuer au moins sur :

- la cartographie logicielle et matérielle du navire,
- la définition des éléments sensible du navire,
- la gestion des vulnérabilités système,

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 techniques relatives à la cyber sécurité du navire.

Autorité nationale en matière de sécurité et de défense des systèmes d'information, l'Agence Nationale de la Sécurité des systèmes d'Information (ANSSI) constitue un réservoir de compétences qui met son expertise et assiste les administrations et les opérateurs d'importance vitale.

Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux, et contribue au développement de la confiance dans le numérique.

Le centre de transmission gouvernemental, placé sous l'autorité du SGDSN, assiste l'ANSSI à travers la mise en œuvre les moyens sécurisés de commandement et de liaison nécessaires au président de la République et au Gouvernement. L'ANSSI bénéficie également de l'expertise d'un comité stratégique constitué de responsables de haut niveau de l'administration, qui propose la stratégie de l'État en la matière.

Trois guides pour la sensibilisation des compagnies et des marins ont été rédigés et sont disponibles gratuitement sur site du ministère (https://www.ecologique-solidaire.gouv.fr/surete-des-navires-et-surete-portuaire):

- « *Cybersécurité : Evaluer et protéger le navire* »
- « *Cybersécurité : Renforcer la protection des systèmes industriels du navire* »,
- « *Guide des bonnes pratiques de sécurité informatique à bord des navires* ». Ce dernier document a été rédigé avec le concours de l'ANSSI et de plusieurs compagnies françaises.

Un autre guide a été rédigé par la gendarmerie maritime pour donner les lignes directrices sur comment agir si une attaque cyber se produit :

- « Guide sur la préservation des traces et indices »

La formation initiale des officiers de la marine marchande intégrera 12 heures de cours destinés à la problématique de cyber sécurité à compter de l'année 2017/2018. Le périmètre de la formation continue reste à définir en fonction de l'expression des besoins des compagnies françaises.

La directive NIS n'a pas encore été transposée par la France. Suite à l'adoption du Livre Blanc sur la défense, il existe déjà une liste française d'« opérateurs d'importance vitale », mais elle est confidentielle.

MISE EN ŒUVRE /FEUILLE DE ROUTE POUR ARMATEURS DE FRANCE :

Armateurs de France a inclus la cybersécurité dans les sujets suivis à partir de 2015. La prise de conscience a eu lieu lorsque s'est posée la question de l'inclusion du maritime dans la directive NIS. Notre action prend deux directions, qui sont complémentaires :

1) **Auprès de nos adhérents** : veille règlementaire, sensibilisation au sujet, diffusion des recommandations des instances et organisations professionnelles internationales et de l'administration française, mise en contact avec l'administration :

Instance compétente : COPIL sécurité-sûreté. Le sujet a ainsi été abordé lors des comités du 6 novembre 2014, 6 mai 2015, 20 octobre 2015, 10 mars 2016, 29 mars 2017 et 28 juin 2017. Si besoin, il pourra

également figurer à l'ordre du jour d'un comité de liaison armateurs/assurance.

Diffusion des guidelines BIMCO, des guidelines de l'ANSSI

2) **<u>Auprès de l'administration</u>**, pour relayer les préoccupations des armateurs et nous assurer de la bonne prise en compte des spécificités maritimes.

Contacts réguliers avec l'ANSSI, y compris visite d'un site.
Participation aux ateliers cybersécurité du Cluster.

Lors de la réunion du 25 janvier 2017 à laquelle participaient le BEAMER, le SGMER, l'ENSM, l'ANSSI, la Marine, la Gendarmerie maritime, les départements DST/ DSUT, les affaires maritimes, le CLUSTER MARITIME et Armateurs de France, le plan d'action suivant a été adopté pour l'année 2017, afin d'élever le niveau d'information et de sensibilisation des armements et des marins :

(1) **Présentation auprès de l'OMI d'une seconde soumission relative à la cyber sécurité** : cette soumission vise à amender la circulaire MSC.1-Circ.1526 du 01 juin 2016 afin d'y intégrer les guides de bonnes pratiques (sensibilisation du marin et au risque industriel).

(2) **Réalisation d'un audit de cyber sécurité** : cet audit sera conduit par l'ANSSI à bord d'un navire de charge. L'objectif de cet audit consiste à poursuivre la stratégie de recueil de renseignements sur les vulnérabilisés du navire afin de définir les moyens à engager pour le protéger d'une cyber menace.

(3) **Développer des scénarios d'attaque d'un navire** : ces éléments permettront d'actualiser la matrice d'évaluation du cyber risque pour un navire. Ces scénarios doivent donc refléter au mieux la « réalité métier » . L'idée est de mettre en scène des situations de cyber attaques pour se rendent compte que la menace existe déjà, mais voir à quel point cela peut être couteux et dommageable pour le navire ou la cargaison.

(4) **Formation continue et initiale du marin** : la formation initiale des officiers de marine marchande intégrera lors de la rentrée 2017/2018 un module relatif à la cyber sécurité.

(5) **Poursuite de sensibilisation des compagnies** : un guide des bonnes pratiques relatives au volet judiciaire sera rédigé en concertation avec la gendarmerie maritime, l'ANSSI et la DAM.

PROBLEMATIQUES

- De quel risque cherche-t-on à se protéger ? Il convient de distinguer le scénario de film catastrophe (prise de contrôle à distance du navire qui pourrait être utilisé comme une arme) et la réalité (intrusion dans les systèmes commerciaux et vol de données confidentiels, blocage du trafic, cyber-rançons)
- Que doit-on protéger : le navire et/ou les infrastructures terrestres
- Formation et sensibilisation

Couts : non
Quid des compagnies disposant d'établissements dans plusieurs Etats membres