MEMOIRE

L'assurance maritime face aux risques cybernétiques

Présenté par :

Ibrahima THIAW

Sous la direction de :

M. Olivier LASMOLES

Suffragant :

M. Pascal GIRERD

Année universitaire : **2019-2020**

Université de Lille

Faculté des Sciences Juridiques, Politiques et Sociales

Mémoire pour l’obtention du Master 2 Droit de la Mer et Risque Maritime

L’assurance maritime face aux risques cybernétiques

Présenté par :

Ibrahima THIAW

Sous la direction de :

M. Olivier LASMOLES

Suffragant :

M. Pascal GIRERD

Année universitaire : 2019-2020

La Faculté des Sciences Juridiques, Politiques et Sociales de l'Université de Lille n'entends donner aucune approbation ni improbation aux opinions émises dans le présent rapport. Ces opinions devront être considérées comme propres à leur auteur.

Remerciements

Je tiens d’abord à remercier tout particulièrement mon directeur de mémoire, Monsieur Olivier LASMOLES, pour sa disponibilité et ses précieux conseils qui m’ont servi tout au long de ce travail.

Ma gratitude va aussi à Monsieur Pascal GIRERD pour son enseignement et pour ses encouragements tout au long de l’année.

Mes remerciements le plus sincères à tous les professeurs de ce master, qui nous ont partagé leur savoir, leur expérience et fortifié notre amour du Droit Maritime tout au long de l’année.

Nous tenons à remercier également Yaye Fatou DIOUF pour son soutien, sa relecture, les orientations et les conseils qu’elle nous a prodigué.

Nous avons eu la chance d’échanger avec de très nombreux acteurs du monde des assurances. Nous les remercions très chaleureusement de leurs conseils très précieux.

Enfin je tiens à remercier ma famille, mes amis pour leur soutien sans failles durant mon cursus universitaire que ce papier vient de clore.

SOMMAIRE :

Sigles et abréviations :

AIS – *Automatic Identification System*

AIPD – Analyse d'Impact relative à la Protection des Données

ANSSI – Agence Nationale de Sécurité des Systèmes d'Information

AWS – *Amazon Web Services*

BIMCO – *Baltic and International Maritime Council*

CCR – Caisse Centrale de Réassurance

CMI – Comité Maritime International

CNUCED – Conférence des Nations Unies sur le Commerce et le Développement

DGITM – Direction Générale des Infrastructures, des Transports et de la Mer

DMF – Droit Maritime Français

EVP – Equivalent Vingt Pieds

FFA – Fédération Française de l'Assurance

FGAO – Fonds de Garantie des Assurances Obligatoires de dommages

GIP ACYMA–Groupement d'Intérêt Public – Action contre la Cyber Malveillance

GPS – *Global Positioning System*

IACS – *International Association of Classification Societies*

ICS – *Internation Chamber of Shipping*

ILS – Insurance linked-Securities

INTERCARGO – *International Association of dry Cargo Shipowners*

INTERTANKO – *International Association of Independent Tanker Owners*

ISEMAR – Institut Supérieur d'Economie Maritime

ISM (Code) **–** *International Safety Management*

ISO – *International Organization for Standardization*

ISPS (Code) **–** *International Ship and Port Facility Security*

IUMI – *International Union of Maritime Insurance*

MSC – *Maritime Safety Committee*

NCPO – *National Cyber Policy Office*

NIS – *Network and Information Security*

NIST – *National Institute of Standards and Technology*

OIV – Opérateur d'Importance Vitale

OSE – opérateurs de service essentiels

OMI – Organisation Maritime Internationale

P&I – *Protection ans Indemnity*

RGPD – Règlement Général sur la Protection des Données

PME – Petites et Moyennes Entreprises

RMS – *Risk Management Solutions*

SI – Système d'infromation

SIEM – *Security Information Event Management System*

SOC – *Security Operation Center*

WWW – *World Wide Web*

INTRODUCTION :

« *Aux pirates en mer se sont substitués les hackers. Et ces derniers espèrent tout autant que leurs homologues voler et détourner de leur cadre légal des informations, des données, et des infrastructures, afin d'en faire un usage frauduleux. Si l'utilisation de radars ou la numérisation des plateformes et des infrastructures maritimes facilitent et sécurisent les transports maritimes, et permettent plus globalement une meilleurs efficacité et un rendement amélioré des activités maritimes, l'imbrication du numérique dans le domaine maritime pose néanmoins des questions essentielles en termes de sécurité*[2]. »

Ainsi s'est exprimé, Philippe Vitel, député du Var, lors de la première édition des *« Rencontres Parlementaires Cybersécurité & Milieu Maritime* », en mars - avril 2015. Pour lui, la digitalisation du monde maritime a certes de nombreux avantages tant dans la sécurité et le contrôles des activités que dans la compétitivité. Mais regorge tout de même quelques risques pouvant affecter de manière considérable tout l'économie du secteur.

Aujourd'hui nous vivons dans un monde où les technologies de l'information deviennent de plus en plus omniprésentes dans nos sociétés. C'est ce qui justifie d'ailleurs une émergence d'un nouveau champ de bataille, sans lignes de front clairement déterminées ni combattants blessés ou tués. C'est une guerre numérique, très sophistiqué et maligne qui se déroule dans le cyberespace et dont les soldats sont des hackers. Et comme les autres domaines à forte composante économique, le milieu maritime n'échappe pas à la déferlante numérique[3]. Il est donc nécessaire voir urgent pour le secteur de se préparer pour faire face à ces nouvelles menaces. Ainsi, avec la digitalisation et la forte dépendance aux systèmes informatique (SI), les scénarios les plus pessimistes sont devenus fort probables. Selon le dernier rapport[4] de Hiscox sur la gestion des cyber risques, « *le nombre d'entreprises ayant fait état de cyber incidents est passé de 45% en 2018 à 61% en*

[2] « Autour des Rencontres Parlementaires - Cybersécurité & Milieu Maritime » La lettre cybersécurité et parlement n°4 1ère Edition, Mars - Avril 2015.
[3] *Ibid.* p2.
[4] « La gestion des cyber risques », Hiscox, Rapport 2019.

2019[5] *»*. Cette augmentation des attaques ou des tentatives démontre encore une fois que les entreprises ne sont pas bien préparées pour faire face à ce risque. En France, la dernière étude du Cesin[6], montre certes une baisse des entreprises ayant déclarées des attaques cyber en 2019: 65% en 2019 contre 80% en 2018. Ce qui est néanmoins à nuancer, car les impacts sur le business sont similaire entre 2018 et 2019: 57% ; ce qui se justifie par la nature potentiellement systémique du risque.

Dans un secteur qui représente plus de 90% du commerce mondial, la priorité se tourne sans doute vers la sécurité du navire, et de ses équipements. Or les navires modernes, embarquent de plus en plus de technologies informatisées et automatisées standards et à haut niveau d'intégration pour gérer leurs fonctions primordiales[7]. L'utilisation de la technologie par les compagnies maritimes à bord et terre a de nombreux avantages: réduction des effectifs, accroissement des capacités du navire, augmentation de l'efficacité des opérateurs, réduction des coûts de maintenance, interchangeabilité des équipements[8].

Mais depuis quelques années, on assiste à une recrudescence des attaques cyber dans le milieu maritime. Cette augmentation des cyber-attaques est due à une vulnérabilité des systèmes d'information et de communication, qui utilisent des systèmes d'exploitation tels que Windows ou Linux. Mais aussi une faiblesse des systèmes de contrôle et d'acquisition de données. Ces failles, souvent accrue par la standardisation massive des équipements embarqués et leur complexité croissante, fait que les attaques cyber deviennent de plus en plus fréquentes. Ces attaques affectent non seulement l'économie de l'entreprise, et si beaucoup d'entreprises préfèrent ne pas communiquer les attaques cyber dont elles sont victimes, c'est souvent pour protéger leur image. La majorité des études situent en effet, le coût global de la cybercriminalité entre 100 et 500 milliards par an[9]. Dès

[5] A noter que l'étude concerne que 7 pays dont la France, l'Allemagne, La Belgique, Les Etats-Unis, l'Espagne, le Pays-Bas et le Royaume-Uni.
[6] « Baromètre de la cyber-sécurité des entreprises », Club des experts de la Sécurité de l'Informatique et du Numérique (CESIN), Vague 5 - Janvier 2020.
[7] Benjamin Coste, « Détection contextuelle de cyberattaques par la gestion de confiance à bord d'un navire », Ordinateur et société, Ecole Nationale Supérieure Mines-Télécom Atlantique, 18 Décembre 2018, https://tel.archives-ouvertes.fr/tel-02079063 , p2.
[8] *ibid.* p.2
[9] Sébastien HEON et Didier PARSOIRE, « la couverture du cyber-risque », extrait de la Revue d'Economie Financière, n° 126.

lors, la mise en place d'une bonne politique de gestion de ce « nouveau » risque semble alors primordiale.

Les acteurs du monde maritime doivent alors faire face à ce risque, en renforçant le niveau de sécurisation des systèmes d'information à bord et à terre. Cette sécurisation des navires nécessite la sécurisation des équipements à bord mais aussi de tous les circuits divers pouvant, par le biais de corrélation, affecter l'ensemble du réseau. Toutefois, la complexité du risque cyber fait que les compagnies maritimes, dans un souci de maitrise et de capacité technologique, optent pour un transfert pur et simple du risque vers le marché de l'assurance. L'industrie de l'assurance a un rôle crucial à jouer dans la gestion du risque cyber par les compagnies maritimes. Il est au premier rang dans l'élaboration d'une stratégie permettant de mieux cerner le risque cyber dans toutes ses dimensions et éventuellement proposer une solution assurantielle adaptée aux besoins des armateurs. Ainsi, l'étude de l'assurance maritime des risques cybernétiques nécessite tout d'abord de définir quelques notions phares nous permettant de déterminer l'étendue de l'étude qui sera effectuée sur ce papier.

Dans toutes les places où le mot « Cyber » est soulevé, cela déclenche automatiquement des interrogations. Et comble disait l'autre: « *Apposez-le sur la couverture d'un quelconque ouvrage et ses chances de succès en seront considérablement augmentées*[10] ». Le risque cyber, voilà, ce qui pose des équations à plusieurs inconnus dans tous les secteurs. Cette notion est dans le langage de tous les secteurs d'activité: santé, industrie, services financiers, technologie, média et communication, Organismes public, énergie et bien évidemment les transports.

Dans le contexte du secteur maritime, comme dans tous les autres secteurs, il n'existe pas de définition universelle du risque cyber. Mais l'accumulation des différentes définitions nous permettra peut-être de mieux cerner la notion. Ainsi le risque cyber se définit par certains assureurs comme « *tout risque de perte financière, d'interruption des*

[10] FEREY, G; GROROD, N; LEGUIL, S. *« L'assurance des risques cyber, Comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive?* », Mines Paris Tech, 2017

activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologies de l'information[11]. » Cette définition semble limitée, dans la mesure où elle ne prend pas en compte le facteur humain. Cet aspect est relevé dans le guide établi par le DGITM, en septembre 2016, qui affirme que: « *La cause première des attaques est liée à l'attaquant. Il est cependant à noter que le facteur humain joue la plupart du temps un rôle clé dans le fait qu'une attaque réussisse ou non*[12]. » Le facteur humain est alors souvent, responsable du succès des nombreuses attaques cyber. Profitons de cette occasion pour enlever au risque cyber sa casquette de risque exclusivement malveillant car selon Willis Tower Watson[13], environs 90% des sinistres cyber déclarés *« résultent d'une erreur humaine ou d'un comportement humain* ».

Dans leur mémoire intitulé « L'assurance des risques cyber, comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive? », soutenu en 2017, Gaspard FEREY, Nicolas GROROD et Simon LEGUIL, proposent une autre définition du risque cyber. Selon eux le risque cyber se définit pour une personne physique ou morale comme « *tout risque d'atteinte d'origine immatérielle à la disponibilité, la confidentialité, l'intégrité ou la traçabilité de son système d'information*[14]. »

De son côté, l'OMI n'a pas donné une définition claire mais donne une appréhension du cyber risque de manière globale. Selon elle, « *les cyber-risques permettent de mesurer à quel point une ressource technologique est menacée par une circonstance ou un événement susceptible de se produire qui pourrait entrainer la corruption , la perte, ou l'altération des renseignements ou des systèmes et, par-là, des défaillances opérationnelles et des lacunes en matière de sécurité ou de sûreté*[15]. » On remarque alors qu'il n'y pas une définition du risque cyber qui fait l'unanimité. Mais une

[11] « *Qu'est-ce-qu'un cyberrisque?* », https://www.nbins.com/fr/blog/cyberrisques/qu-est-ce-qu-un-cyberrisque/ {Consulté le 17 Août 2020}.
[12] « *Cyber Sécurité, évaluer et protéger le navire* », DGITM-Direction des affaires maritime, Edition septembre 2016, p13.
[13] « *When it comes to cyber risk, businesses are missing the human touch* », Willis Towers Watson - https://www.willistowerswatson.com/en-BE/news/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch
[14] Op. cit, p17.
[15] http://www.imo.org/fr/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx {Consulté le 17 août 2020}.

chose est sûre, c'est que toutes ces définitions et dans bien d'autres, il y a toujours des éléments de ressemblance sur lesquels on peut se base pour déterminer une définition universelle du risque cyber.

Pourtant l'un des défis des assureurs est de se mettre d'accord sur une définition universelle du risque cyber à l'aide d'informations reçu de part et d'autres des acteurs. Mais la tâches sembles difficiles, c'est pourquoi certaines compagnies d'assurance, dans leur volonté de développé un marché cyber, n'hésitent plus à classer en premier lieu risque « cyber » et ceci bien avant le risque terroriste et de catastrophes naturelles [16]. Cette approche démontre que les assureurs, contrairement aux assurés (compagnies maritimes), dont la plupart considèrent que « *ça n'arrive qu'aux autres* », mesurent l'ampleur de la menace.

Mais cette volonté de développer un marché cyber n'est pas reçue à bras ouvert par tous les acteurs de l'industrie de l'assurance, en raison de sa complexité mais surtout de sa nature systémique, qui peut engendrer des dégâts inassurables. Ainsi on assiste à un éternel débat sur l'assurabilité du risque cyber. Entre ceux qui y voient une opportunité de croissance économique, c'est à dire un marché à très haut potentiel et, ceux qui, plus pessimistes le considèrent comme un terrain inconnu, à très haut risque. L'objectif de ce mémoire n'est pas de se positionner sur ce débat, car la priorité est ailleurs. Il serait plus intéressant de reconnaitre qu'il y a certes des difficultés pour la couverture du risque cyber mais qu'en faisant face à ces problèmes, les acteurs du secteur notamment, les assureurs et les compagnies maritimes peuvent mettre en place des moyens matériels, humains et financiers afin de développer un marché cyber solide et efficace.

Dans le contexte spécifique du monde maritime, où le secteur est fortement cyberdépendant, l'urgence est renforcer la collaboration des acteurs, y compris l'Etat et les Organisations internationales. Mais au lieu d'adapter une « *stratégie de l'autruche* », les acteurs du monde maritime doivent adopter une culture du risque cyber.

[16] « *Cyber Sécurité, renforcer la protection des systèmes industriels du navire* », DGITM-Direction des Affaires Maritimes, Edition janvier 2017, p3.

« *Comment alors placer le curseur afin de prendre toutes les mesures nécessaires, sans pour autant s'engager dans une course à l'échalote, motivée par notre ignorance collective?*[17] » La prise en conscience du risque cyber par les acteurs du monde maritime semble alors acquise, reste à trouver des processus d'identification, d'analyse, d'atténuation et de transfert du risque à un niveau acceptable compte tenu des coûts et des avantages.

La méconnaissance du risque cyber par les assureurs influence-t-elle sur sa prise en charge? Si tel n'est pas le cas, quelles stratégique assurantielles doit être adapter par l'industrie de l'assurance pour préparer la cyber-résilience des compagnies maritimes? En d'autres termes comment les assureurs entendent-ils intégrer le risque cyber dans leur gestion des risques?

Pour tenter de répondre à cette question, il nous semble judicieux de détecter dans un premier temps les difficultés qui empêchent les assureurs de convaincre leur réticence pour le risque cyber. Dans toutes les conférences ou séminaires dont le thème est l'assurance des risques cyber, à l'unanimité, les acteurs reconnaissent leur manque d'information pour le risque cyber. Ce manque de données pour le risque cyber rend certains assureurs dubitatifs sur l'avenir du marché. Ils considèrent que c'est une marché en devenir. C'est la raison pour laquelle, de nombreux acteurs commencent déjà à déceler les problèmes qui affectent l'assurance de ce risque.

C'est ce dont nous allons parler dans la première partie de ce mémoire: la problématique de l'assurabilité du risque cyber (**Partie I**).

Dans cette première partie nous allons essayer repérer les différentes sources de problème qui retardent le développement du marché de l'assurance cyber. Une fois le problème détecté, les acteurs vont essayer d'apporter des solutions adaptées. Il sera intéressant de faire une analogie comme dans le domaine de la santé. Les spécialistes, une

[17] « *Autour des Rencontres Parlementaires », Op. cit.*

fois le virus découvert, essayent de lutter contre cette ennemie invisible. Le premier acte en général est la création de « centres d’expertise, comme l’Institut Pasteur en 1888, qui visaient à disposaient des meilleurs experts et installations pour mener la lutte. C’est exactement la même chose pour la prise en charge d’un « nouveau » risque. Une fois détecté, les assureurs avec l’aide des assurés, peuvent s’engagent à relever des défis pour apporter des solutions assurantielles adaptées aux besoins des clients.

Ce sera l’objet de la deuxième partie de ce papier: l’engagement des assureurs pour la prise en charge du risque cyber par les assureurs (**Partie II).**

PARTIE I. LA PROBLÉMATIQUE DE L'ASSURABILITÉ DU RISQUE CYBER

CHAPITRE 1ER. LE RISQUE CYBER : UN RISQUE NOUVEAU DANS LE SECTEUR MARITIME

Nombreux sont les acteurs qui pensent que la couverture du cyber risque est encore prématurée, en raison du manque de données. La découverte de ce risque technologique (**Section1**) par le secteur maritime s'est faite à la suite des nombreuses attaques d'une gravité extrême dans l'économie des victimes. C'est ainsi que son transfert vers les assurances s'est avéré urgent. Ce transfert vers l'assurance sera facilité par une réglementation (**Section 2**).

SECTION 1 : A LA DÉCOUVERTE D'UN RISQUE TECHNOLOGIQUE

Le cyber risque est un risque qui touche toutes les entreprises de tous les secteurs d'activité. Comme dans le terrestre ou l'aérien, ce risque commence à inquiéter sérieusement le secteur maritime depuis quelques années. De ce fait, la réaction du monde maritime doit se faire de manière organisée pour déceler toute la particularité de ce risque (**Sous-section 1**). Mais s'il y a un écueil qui coupe l'appétit des assureurs pour la couverture de ce risque c'est bien sa nature systémique (**Sous-section 2**).

Sous-section 1: La particularité du risque cyber

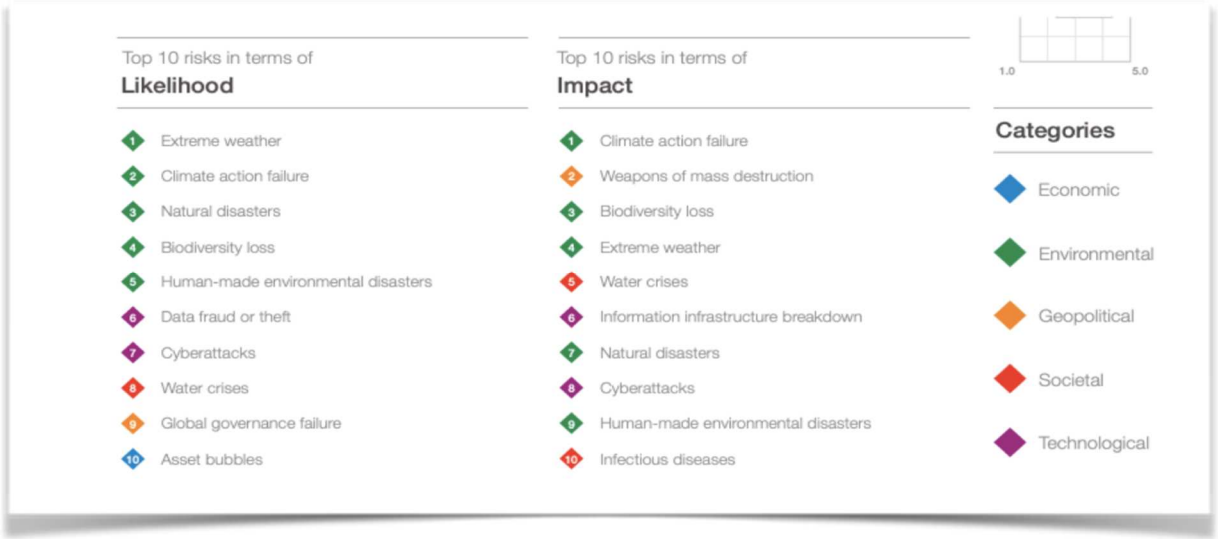
Comme précisé par la fédération française des assurances dans sa « cartographie 2020 sur les risques émergents »: « *le risque cyber (3,8; 3,5)* [18]*demeure à court terme le risque principal pour les sociétés d'assurance et de réassurance, comme lors des deux premières éditions. L'intensification des cyber attaques, en nombre et en exposition, la multiplication de leur formes et l'augmentation de la vulnérabilité (voitures autonomes, pacemakers, internet des objets...) accroit à la fois l'impact potentiel de ce risque mais aussi sa fréquence.* » Cela veut dire que le risque cyber est et reste de loin le risque moderne le plus redouté. C'est ce que nous allons démontrer avec quelques chiffres marquants (A) avant de voir son caractère systémique (B).

[18] Le score (probabilité; impact) a un minimum de (0; 0) et un maximum de (5; 5)

A) Quelques chiffres marquants

Le cyber risque est relativement récent. Il est sans doute l'un des risques majeurs du XXIe siècle en raison de son caractère universel et complexe. De plus en plus d'experts tirent la sonnette d'arme sur l'impact progressif des risques technologiques. Dans la 15ème édition du rapport annuel du *World Economic Forum*, le risque cyber est classé 7ème sur les 10 risques mondiaux qui peuvent avoir un impact important au cours des 10 prochaines années. Cette étude marque l'importance capitale pour les acteurs économiques de protéger leurs systèmes informatiques (SI) contre les risques cyber très dommageables. Ce rapport identifie les principales menaces auxquelles le monde doit faire face selon la probabilité et l'ampleur de leur impact.

Figure 1: Ci-dessous un tableau où vous remarquerez que le risque cyber est placé 7ème rang par la probabilité et 8ème rang par l'impact selon la perception de multiples stakeholders, sur le long terme.



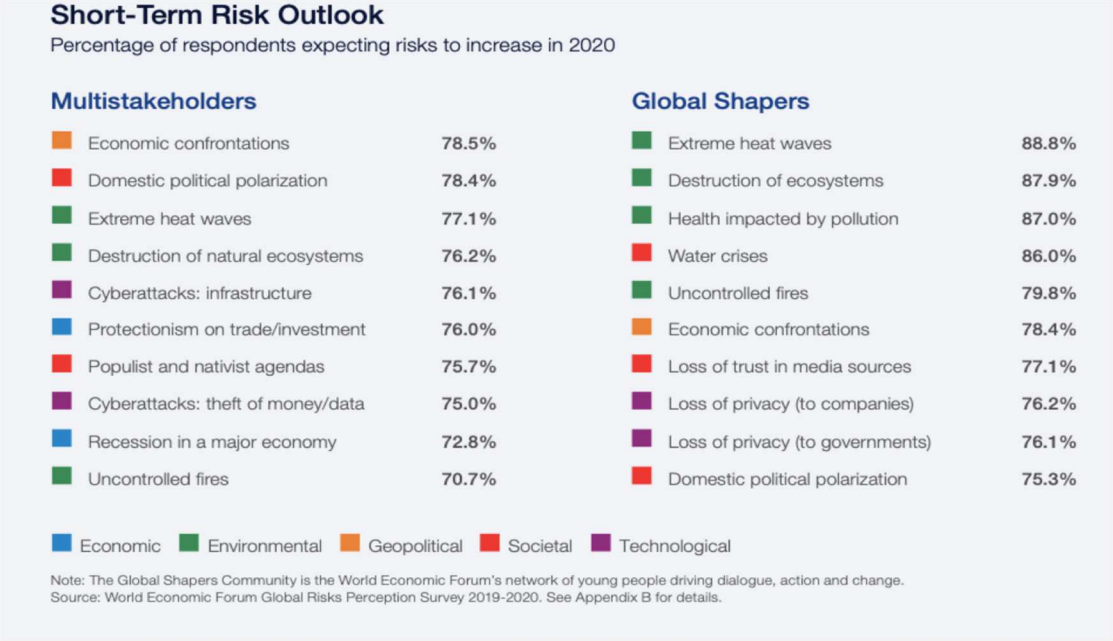
Source: World Economic Forum Global Risks Perception survey 2019-2020.

Cette enquête montre que le risque cyber, au-delà des questions liées au réchauffement climatique, est la principale menace en termes de probabilité au cours de la prochaine décennie. C'est une étude dans le long terme. Mais qu'en est-il de la menace dans le court terme surtout avec la récente crise sanitaire qui a sans doute augmenté la probabilité d'occurrence du risque cyber avec l'utilisation du télétravail. Il est peut-être

trop tôt de faire une analyse globale de l'impact de la crise en terme de cyber attaque. Notons seulement qu'il y a de nombreux cyber attaques pendant la crise sanitaire. Par exemple dans le secteur des transports à l'image de MSC, dans le maritime, en Avril 2020 ou de EasyJet[19], dans l'aérien, en janvier 2020.

Dans le rapport de *World Economic Forum* de 2020, on remarque qu'il y a une élevation du niveau de conscience du risque cyber. Les acteurs économiques deviennent de plus en plus inquiets à la question des risques technologiques. Dans ce rapport, on remarque que le paysage des risques mondiaux et leurs interconnexions s'accumulant depuis plusieurs années, commencent à se faire sentir.

Figure 2: Ci-dessous, un tableau décrivant le pourcentage de personnes qui pensent qu'un risque va augmenter au cours des 10 prochaines années.



Source: World Economic Forum Global Risks Perception Survey 2019-2020.

[19] http://cyberguerre.numerama.com.via.snip.ly/obt3e4#https://cyberguerre.numerama.com/5194-easyjet-2-200-cartes-de-credit-divulguees-et-9-millions-de-clients-touches-dans-une-cyberattaque.html

Selon cette étude, 76,1% des personnes interrogées pensent que le cyber attaque sur les infrastructures va augmenter au cours de la prochaine décennie; et 75% d'entre eux pensent que les pertes de financières et de données vont augmenter dans les 10 prochaines années. On voit nettement que le risque cyber est au podium des 5 risques mondiaux dont la probabilité d'occurrence est élevée et que son évolution dans le temps risque de bouleverser l'économie mondiale.

Le monde maritime n'est pas à l'abri de cette menace car il migre de plus en plus dans la numérisation; ce qui est l'un des facteurs clé de potentiels attaques-cyber.

Parallèlement, la Fédération Française de l'Assurance, a récemment publié une cartographie des risques émergents[20] pour la profession de l'assurance et de la réassurance. Cette étude montre que sur 23 risques émergents considérés comme pouvant avoir un impact sur le monde de l'assurance et de la réassurance en France, le cyber attaque est au premier rang avec une probabilité d'occurrence de 3,8/5 et un impact 3,5/5 sur un an. Le score est encore plus élevé sur 5 ans avec une probabilité d'occurrence et d'impact potentiel plus important. **(Voir annexe 1).**

Au-delà de ces chiffres, il faut noter que la problématique d'assurabilité du risque cyber réside surtout dans sa nature systémique.

B) La nature systémique du risque cyber

Le risque cyber est un risque potentiellement systémique[21]. Assez récent, le risque cyber s'apparente comme un risque de nature à s'étendre de manière exponentielle sur un ensemble de système. Dans son rapport sur l'évolution des risques du système financier français publié en décembre 2019, la banque de France met en évidence que la digitalisation renforce à la fois « l*e risque d'un incident cyber et son impact potentiel tant pour les institutions et les infrastructures financières immédiatement touchées que pour le système financier dans son ensemble*[22]»; avant de conclure que « *le risque cyber n'est plus un risque opérationnel idiosyncratique, il devient potentiellement systémique*. »

[20] Cartographie 2020 des risques émergents pour la profession de l'assurance et de la réassurance, FFA.
[21] Wissem Ajili Ben Youssef, les cyber risques: Nature, Etendue et moyens de couverture, Lamy, Droit et Patrimoine, n°298, 1er janvier 2020.
[22] Banque de France, Evaluation des risques du système financier français, décembre 2019, p40

Cette approche du risque cyber montre que la numérisation des infrastructures participe rigoureusement à la vulnérabilité des systèmes et à l'accroissement des conséquences d'un risque cyber.

La notion du risque systémique n'est pas simple à définir dans sa globalité mais à travers la définition de la crise systémique[23], le risque systémique est appréhendé comme « *un risque de dégradation brutale de la stabilité financière, provoquée par une rupture dans le fonctionnement des services financiers, et répercuté sur l'économie réelle*[24]. »

Dans le domaine maritime ce risque est un réel problème dans la mesure où il y a une interconnexion standardisée et peu sécurisée des systèmes informatiques. De plus on assiste à une cyber-vulnérabilité exposant les appareils de plus en plus à des attaques cyber. Cela est dû à la diffusion ubiquitaire du numérique dans les navires qui pourrait causer des incidents affectant un nombre considérable d'acteurs économiques (qui peut même dépasser les frontières), portant les indemnisations à des montants qui peuvent menacer la résilience des souscripteurs. En plus, en raison de la nature mouvante du risque cyber et de sa méconnaissance par les acteurs économiques, les assureurs maritimes font face à un risque qui ne stimule pas leur appétit.

Le cyber risque serait donc « *un risque systémique qui se dessine au-delà des frontières géographiques mais dont les modes de propagations et d'agrégation sont loin d'être maîtrisés*», souligne Wissem Ajili Ben Youssef[25].

Pour les assureurs, le risque est trop grand car une attaque cyber peut affecter plusieurs assurés en même temps, provoquant ainsi une demande d'indemnisation à très grande échelle que les assureurs ne pourront pas satisfaire. Un tel scénario est à prévoir du fait que les armateurs utilisent les mêmes plateformes portuaires; et dans ce cas d'espèce le risque peut émaner de partout. Par exemple, dans le cadre d'une attaque cyber qui cible un

[23] Définition donnée dans « Guidance to Assess the Systemic importance of financial institutions, markets and instruments », 20 octobre 2009, FMI, BRI, CSF

[24] Jean-François Lepetit, Rapport sur le risque systémique, Ministère de l'Economie, de l'industrie et de l'emploi, avril 2010, p12.

[25] Wissem Ajili Ben Youssef, Les cyber risques: Nature, Etendue et moyens de couverture, Lamy, Droit et Patrimoine, n°298, 1er janvier 2020.

port fréquenté par plusieurs armateurs, le virus peut se propager via les échanges entre le port et les navires et qui par la suite s'étend sur plusieurs acteurs économiques. Les conséquences d'un tel scénario peuvent être phénoménales. Reste à savoir si les assureurs pourront évidemment assimiler les différents niveaux de responsabilité et satisfaire un besoin d'indemnisation à très grande échelle.

Il est donc important d'être explicite pour apporter une solution assurantielle attirante. Car l'ambiguïté qui règne au sujet du risque cyber, ne profite ni aux armateurs, qui sous-estiment l'impact potentiel d'une attaque cyber dans leur économie, ni aux assureurs, qui ne disposent pas pour le moment de l'abc du risque cyber potentiellement systémique. La solution à cette situation se trouve naturellement dans le dialogue entre assurés, et assureurs, que nous verrons dans la deuxième partie de ce mémoire. On se demande tout de même si l'ACPR[26], n'a pas un rôle à jouer dans la gestion du risque cyber, en imposant aux assureurs de connaître leur exposition au risque cyber et à proposer un produit assurance cyber clair.

Les difficultés de maitrise du risque cyber par l'industrie maritime sont dues en grande partie par une ignorance, pendant longtemps du risque. Mais depuis quelques années on remarque une prise de conscience du risque cyber, qui est certes forcée par la répétition des attaques cyber.

Sous-section 2: La prise de conscience forcée de l'industrie maritime

Le risque cyber est l'un des risques émergents des 10 prochaines années. Dans le monde maritime, on assiste depuis quelques années à une recrudescence des attaques cyber (A) avec une évolution des pertes constatée (B).

A) La recrudescence accrue des incidents cyber

Le Bureau Maritime International (BMI) disait que « *le transport et la logistique maritime sont le prochain terrain de jeux des pirates informatiques.* » le BMI a tiré la

[26] Autorité de Contrôle Prudentiel et de Résolution

sonnette d'alarme depuis 2014, en appelant le secteur maritime à se protéger contre les attaques cyber. La digitalisation n'a pas que des bienfaits. Aujourd'hui il est possible pour un hacker de dérober des données ou de détourner un navire à distance ou même son système d'armement.

Il existe deux principales menaces: l'espionnage et le sabotage. L'espionnage, qui consiste par exemple à voler des données techniques pour connaître avec précision le trajet d'un navire. Pour Dominque Riban[27]« *cela permet à un concurrent de voler le marché et de pratiquer des prix plus bas* ». Mais cela n'est rien à côté des risques cyber encourus par les géants de mers et l'industrie maritime de manière globale. Les conséquences d'un piratage informatique sont d'une extrême complexité.

En 2011, le port d'Anvers a été la cible d'une attaque. Les attaquants ont ciblé des agents portuaires via un malware pour récupérer un mot de passe contrôlant l'accès au système de gestion des conteneurs. Les trafiquants ont ainsi pu repérer des conteneurs potentiellement intéressants du fait de leur trajet, puis charger et décharger de la drogue en toute discrétion.

En août 2012, la compagnie pétrolière saoudi Aramco, a été victime d'une cyberattaque, le contenu de plus de 35.000 ordinateurs ayant été purement et simplement effacé. La compagnie incapable de facturer le pétrole quittant ses raffineries, du fait qu'elle ne disposait plus d'information sur les acheteurs.

Mais la plus grande attaque cyber ayant touchée le monde maritime reste celle de *Notpetya,* en juin 2017. Cette attaque cyber dont la cible était les entreprises Ukrainiennes est devenue hors de contrôle et s'est très rapidement répandue dans le monde entier. Le groupe AP Møller-Mærsk, a été la cible maritime de l'attaque du *Notpetya*[28], qui a, par ailleurs touché plusieurs ports de commerce dont ceux de Rotterdam, de New York, et de Mumbai. Cette attaque aurait coûté plus de 300 millions de dollars au groupe Maersk et entrainé la destruction de dizaines de milliers d'ordinateurs lui appartenant. Au total, 4000

[27] Directeur de l'Agence Monégasque de Sécurité Numérique, ancien directeur général adjoint de l'ANSSI.
[28] Notpetya, 2017

serveurs, 45000 ordinateurs et 2500 applications ont été détruits. Cette attaque a été la pire que le monde maritime ait connu jusqu'ici. L'ampleur de cette attaque a montré la vulnérabilité des acteurs maritimes face aux risques cyber. Notons aussi l'attaque du *WannaCry*[29], dans la même année, qui a affecté la planète entière et a coûté aux acteurs économiques des milliards de dollars. Tout de même, les attaques cyber continuent à se répéter dans le secteur. En juillet 2018, Cosco avait été victime de malware dans le port de Long Beach. Il y a aussi l'attaque contre le port américain de San Diego en octobre dans la même année, tout comme celle contre Clarkson, spécialiste courtage maritime et de la recherche, en novembre 2018, impliquant un accès non autorisé aux systèmes informatiques de l'entreprise ou celle contre le fournisseur anglais de service maritime James Fisher &Sons à la suite d'une intrusion, en novembre 2019.

La plus récente, avril 2020, est celle contre le centre de données du groupe MSC, à Genève, qui a contraint le groupe à restreindre l'accès à son site internet pendant quelques jours[30] .

Toutes ces attaques cyber, ont poussé l'organisation des armateurs danois (Danish Shipping) à mener une enquête. Le résultat de cette enquête a démontré que 42% des cadres supérieurs indiquent qu'ils sont très inquiets ou extrêmement inquiets que leur entreprise soit attaquée ou que leurs données soient perdues dans les 12 prochains mois. Par conséquent, de plus en plus de compagnies maritimes augmentent leur budget pour la sécurité informatique.

Selon la directrice exécutive de Danish Shipping, Maria Skipper Schwenn « *la cible des cyberattaques étaient dirigées contre les systèmes terrestres des compagnies maritimes et non contre les navires en mer* », mais aujourd'hui on remarque que la sophistication des attaquants de plus en plus élevée, permet d'attaquer les systèmes informatiques à terre mais aussi à bord des navires allant même parfois jusqu'au détournement.

[29] WannaCry, Mai 2017

[30] Notons que MSC dans un communiqué du 15 avril 2020 a précisé que « tous les systèmes sont à nouveau pleinement fonctionnels (...) et ne manquerons pas de vous tenir informés de ses conséquences ». Reste à voir s'il s'agit d'une vraie cyberattaque ou d'une simple défaillance technique due à l'activation de tous les outils techniques dans un contexte de crise sanitaire.

B) L'évolution des pertes liées aux cyber-risques

L'industrie maritime a perdu beaucoup de temps avant de parler des risques cyber. Il a fallu une répétition des attaques de plus en plus intenses et de plus en plus désastreuses tant financièrement que matériellement pour évoquer sérieusement la question. Mais l'impact des incidents cyber ne se limite plus à la gestion de la perte ou du vol de données. Depuis quelques années, on constate un accroissement des inquiétudes à l'égard des cyber-risques. Les préoccupations des acteurs maritimes s'étendent aussi aux atteintes à la propriété et à la réputation ainsi qu'aux coûts liés à la perte d'exploitation voir même à une grave perturbation. Il faut aussi noter les pertes peuvent provenir d'une attaque cyber intentionnelle, d'une erreur humaine involontaire ou d'un bug informatique.

Dans une étude publiée dans le *Journal of Cybersecurity*, en août 2016, l'auteur estime le coût moyen d'une atteinte à la protection des données à 200.000 USD par entreprise[31]. Il estime en effet que le coût des incidents cyber n'est pas aussi élevé contrairement à ce que les enquêtes en révèlent. Mais il faut se rappeler que le risque cyber est un risque qui se transforme vite, avec une nature systémique dont les conséquences peuvent dépasser les frontières. L'évaluation de l'impact d'un incident cyber doit inclure non seulement les coûts de la perte d'exploitation mais aussi les coûts générés par l'atteinte à la réputation, à la perte de client futur et les pertes liés aux dégâts matériels. Selon une étude de l'institut Ponémon, la perte d'informations est la conséquence la plus coûteuse d'un incident cyber avec 39% du coût, suivi de la perte d'exploitation avec 36% du coût. Cela inclut la perte de productivité des employés et la défaillance des processus commerciaux après une attaque. La perte de revenus et les dommages aux équipements viennent ensuite, avec 20% et 4% respectivement[32].

En 2015 le Lloyd's of London avait estimé le cout des cyber-attaques à 400 milliards de dollars pour les entreprises par an[33]. Ce montant inclut les dommages liés à

[31] Sasha Romanosky, « Examining the costs and causes of cyber incidents », Journal of Cybersecurity, Vol.0, No.0, Août 2016, p2.
[32] 2016 Cost of Cyber Crime Study & the Risk of Business Innovation, Ponemon Institute, Octobre 2016, p2.
[33] https://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

l'incident mais aussi à la perturbation du cours normal des affaires consécutives aux attaques. Les conséquences d'une attaque cyber dans le secteur maritime peuvent parfois dépasser les estimations. En effet lorsque qu'une compagnie maritime est victime d'une attaque cyber, tout le système d'exploitation est perturbé et cela peut engendrer, au-delà des pertes d'exploitation, des pertes de bénéfices à cause d'investissements déférés, des coûts d'opportunité en temps et en ressources pour réagir contre l'attaque. Tout cela nécessite une bonne couverture cyber pour se prémunir de ces éventuelles conséquences économiques.

De plus, la récente attaque contre le géant maritime Maersk a fait comprendre à l'ensemble de l'industrie maritime qu'il est également exposé aux cyber-risques au même titre que l'aérien ou le terrestre. D'autant plus que les compagnies maritimes ont des systèmes d'information reliant la mer et la terre. Il serait mieux d'anticiper la cyber-résilience des compagnie des assureurs; même s'il s'avère vrai que le risque cyber est un risque complexe et très évolutif. Toutefois, avec une réglementation bien établie qui aiderait les assureurs à mesurer la capacité de gestion du risque cyber par les compagnies, le secteur maritime peut éviter les conséquences désastreuses des cyber-attaques constatées ailleurs.

SECTION 2: BREF ÉTAT DES LIEUX SUR LA RÉGLEMENTATION RELATIVE AU RISQUE CYBER

La couverture d'un risque nécessité forcément un encadrement réglementaire dont le respect aiderait assuré et assureur à mieux le cerner. La règlementation est un outil crucial pour la viabilité d'un marché. C'est pourquoi on constate une réglementation qui se développe au niveau Européen (**Sous-section 1**). Mais comme ce risque est universel, les organisations internationales ont également apporté leur aide dans la règlementation (**Sous-section 2**).

Sous-section 1: Une réglementation en expansion en Europe

La réglementation pourrait être une clé fondamentale dans la prise en charge du risque cyber par les assureurs. Ces derniers ont besoin d'une réglementation protectrice et encourageante, leur permettant de mieux cerner ce risque et de proposer un produit

assurantiel adapté. Il existe une réglementation au sein de l'union (A) mais la France a aussi établi une réglementation (B) dans ce domaine.

A) L'environnement réglementaire du risque cyber au sein de l'UE

La croissance des risques liés à l'évolution des nouvelles technologies de l'information et de la communication et à l'accroissement de leur utilisation nécessite encore la mise en place d'un cadre juridique adapté. Au sein de l'union, nous avons la récente directive de Nis de 2016 (1) et le Règlement Général sur la Protection des Données de 2016 (2).

1) La Directive Nis, décret d'application 23 mai 2018

La directive NIS[34] relève la problématique des réseaux et des SI ainsi que la nécessité d'apporter une réponse unifiée aux risques qui peuvent affecter les entreprises et leur niveau de cybersécurité. A l'échelle européenne, cette directive détermine des obligations à destination des Etats et des opérateurs. Et c'est l'article 14 alinéa 1 de la directive qui prévoit que « *Les États membres veillent à ce que les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances* ». Cette disposition recommande aux Etats membres de contrôler si les opérateurs de service essentiels (OSE) ont pris toutes les mesures préventives nécessaires pour limiter les risques technologiques auxquels ils peuvent faire face.

Les OSE sont définis comme des acteurs dont l'interruption de leur service pourrait avoir un impact significatif sur le fonctionnement de l'économie ou de la société. Ceci montre l'importance capitale de ces OSE mais également l'ampleur que peut avoir une attaque cyber sur ces derniers. L'alinéa 3 du même article rajoute que « *Les États membres veillent à ce que les opérateurs de services essentiels notifient à l'autorité*

[34] Directive NIS (UE) n°2016/1148 du Parlement européen et du conseil du 06 juillet 2016 relative aux mesures destinées à assurer un niveau élevé et commun de sécurité des réseaux et des systèmes d'information (SI) dans l'Union

*compétente ou au CSIRT, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Les notifications contiennent des informations permettant à l'autorité compétente ou au CSIRT de déterminer si l'incident a un impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine***. »** En d'autres termes les OSE ont l'obligation de notifier, sans délai, à l'autorité compétente ou au CSIRT[35] tout incident de nature à compromettre la continuité des services essentiels. Les compagnies de transport maritime et les gestionnaires de ports sont soumis à ces dispositions.

En France, la directive a été transposée dès 2018 avec le décret d'application en date du 23 mai 2018[36]. Ce décret d'application concerne aussi le secteur d'activité des transports. Et pour le transport maritime il y a une liste des opérateurs et services essentiels concernés. Ils vont devoir se conformer à un certain nombre de règles et les appliquer. A défaut, la responsabilité de l'armateur pourrait être engagée. Et quand on parle de responsabilité on a tendance à se tourner vers les assureurs.

Cette nouvelle réglementation va permettre aux entreprises d'avoir une meilleure analyse des risques cyber en pleine coopération avec les assureurs puisqu'il peut y avoir des sanctions en cas de non-respect des règles. C'est pourquoi il est important d'échanger avec les assurés et voir de quelle manière leur exposition aux risques cyber est la plus faible possible. Mais au-delà de la Directive, il existe un règlement essentiel pour la protection des données dont le bilan de son application reste encore insatisfaisant.

2) Les difficultés d'application du règlement RGPD

Si la question de la sécurisation des navires peut obtenir une réponse avec l'adoption de la directive de NIS, il n'en est pas pour autant pour les assureurs, qui, au-delà

[35] Computer security Incident response team (CSIRT) est un centre d'alerte et de réaction aux attaques informatiques, destinés aux entreprises ou au administrations, mais dont les informations sont généralement accessible à tous.

[36] Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

de la complexité de traitement du risque cyber, doivent se conformer aux obligations du règlement général sur la protection des données (RGPD[37]).

Le monde du transport maritime s'est métamorphosé avec l'internet. Ce qui est certes une avancée considérable pour la compétitivité et la concurrence mais rend de plus en plus vulnérable les systèmes d'information des compagnies maritime notamment leur base de données. Les assureurs, dont la mission principale est caractérisée par le traitement de données à caractère hautement personnel, sont concernés au premier chef. Le règlement RGPD oblige « le responsable du traitement » (l'assureur) à effectuer des analyses d'impact relative à la protection des données (AIPD). Selon l'art 35 du règlement : « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, […] est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. ».* Cette disposition peut s'avérer contraignante pour les assureurs dans la prise en charge du risque cyber. Contrairement aux risques traditionnels, qui certes nécessitent la communication de certaines informations à caractère personnel, la prise en charge du risque cyber nécessite une communication plus large de données à caractère confidentiel en raison de l'objet même de la protection qui est celle des systèmes informatiques.

Dans une récente enquête effectuée par *Optimind,* on remarque que (sur 50 répondants) seul 50% des assureurs interrogés déclarent des AIPD en cours de réalisation pour des traitements prioritaires et seuls 21% d'entre eux ont terminé leur AIPD[38]. Le groupe estime que « l*es principales difficultés portent à plus de 60% sur l'évaluation de la gravité et de la vraisemblance pour déterminer le niveau de risque.* » Cela montre nettement les difficultés des assureurs à se conformer aux obligations du règlement RGPD. D'autant plus que Sanaa Nouiri, Senior manager risk chez Optimind expliquait que « *les*

[37] Règlement (UE) 2016/679 du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), du 27 avril 2016

[38] RGPD: Analyse d'impact des traitements sur les données personnelles: AIPD. Où en êtes-vous?, Optimind, 2019.

difficultés rencontrées par les assureurs sur la mise en œuvre des AIPD sont révélatrices des difficultés rencontrées en général pour se conformer aux obligations du RGPD.»

Par ailleurs, il existe en droit Français une action de groupe permettant à une personne de mandater un organisme habilité pour demander réparation lorsqu'il estime que ses droits ont été violés dans le cadre de la protection des données à caractère personnel. Cette action est prévu par le règlement RGPD dans son article 80 intitulé « *représentation des personnes concernées* ». Dans le rapport[39] publié en janvier 2018, le Club des juristes estime que « *cette nouvelle pratique présente un véritable enjeu pour le développement de l'assurance du risque cyber*. » D'autant plus que le risque cyber dans sa globalité peut paraitre extrêmement risqué à assurer dans la mesure où plusieurs dommages peuvent naitre du seul fait de l'attaque. Pourtant l'article 43 ter de la loi informatique et liberté de 1978, introduit dans la loi de modernisation de la justice de 2016, prévoit que cette action ne peut être exercée que pour faire cesser les manquements aux règles en matière de protection des données. Ce qui veut dire que « *l'action de groupe en matière de protection des données à caractère personnel ne permet donc pas de demander réparation des préjudices subis.* » argue le club des juristes dans son rapport.

B) L'environnement réglementaire du risque cyber en France:

Dans le cadre de la réglementation en matière de données et de sécurité des systèmes informatiques, la France a engagé une politique depuis de nombreuses années avec la loi relative à l'informatique, aux fichiers et aux libertés de 1978 (1) et la loi de programmation militaire de 2013, qui est le fondement de la Directive NIS (2).

1) La loi de 1978 sur la liberté informatique

Il est important noter que la France est en avance sur la protection des données et des SI, notamment avec l'ANSSI qui pilote tous ces sujets. Il est complexe pour les armateurs de faire une approche globale du risque cyber et de transférer ce risque aux assureurs mais l'un des points clés c'est la réglementation. La législation française en matière de protection des données et de sécurité des S.I impose pour certains opérateurs

[39] Club des juristes, Assurer le risque cyber, Janvier 2018, Tome I, p64

comme les opérateurs d'importance vitale (OIV), une obligation de notification à l'autorité compétente de l'incident en question. Cette notification, en France, doit être effectuée auprès de l'ANSSI[40] en cas d'incident sur les S.I.

Dans le secteur maritime les acteurs manipulent des données à caractère personnel et confidentiel, ce qui augmente le risque d'intrusion par le biais des échanges électroniques. Ce risque nouveau peut entrainer des atteintes aux données personnelles des tiers et de l'entreprise, ou des pertes d'exploitation consécutives qui ne sont pas pris en charge par les contrats traditionnels.

2) La loi de programmation militaire 2013

Parallèlement, la France a, à travers la loi de programmation militaire de 2013 et ses textes d'application[41], imposé aux opérateurs d'importance vitale (OIV) du transport maritime les dispositions de ladite loi. En effet les OIV, dont la liste n'est pas accessible au grand public, certainement pour des raisons de sécurité nationale, sont définies par l'article L1331-1 du code de la défense comme « *les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative* ».

Dans le transport maritime, les OIV doivent respecter, à leur frais, des règles de sécurité visant à protéger leurs systèmes d'information pour faire face aux menaces cyber et répondre aux besoins de la sécurité nationale. Ils doivent mettre en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes informatiques. Ces systèmes de détection doivent être exploités exclusivement par un

[40] Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)

[41] En l'occurrence, le décret n°2015_351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale, et l'Arrêté du 11 août 2016 fixant les règles de sécurité et les modalitéss de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous- secteur d'activités d'importance vitale « Transports maritime et fluvial » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense– JORF du 25 août 2016 ».

prestataire de service qualifié dont la liste est prévue par l'ANSSI[42]. A l'heure actuelle, plus d'une centaine de services sont qualifiés pour la détection d'incidents de sécurité.

Notons que la réglementation nationale a également intégré les exigences spécifiques du code ISPS[43] dans la division 130 annexée à l'arrête de 1987 relatif à la sécurité des navires (art 130-39). Aux termes de ses dispositions, la France impose aux armateurs d'évaluer le risque cyber et de mettre en place de nouvelles mesures, notamment sur le plan de sûreté du navire[44]. Selon Armateur de France, ce plan de sûreté du navire définit les procédures à appliquer pour chaque risque identifié pour statuer au moins sur:

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

Cette évaluation est d'une importance capitale car elle peut permettre de connaître le seuil de probabilité d'accident, les systèmes clés du navire, les conditions d'ordres politique et technique relatives à la cybersécurité du navire. De là, les assureurs conscients de l'ampleur et de la profondeur de la menace, peuvent avoir confiance aux assurés pour la couverture des risques cyber dans la mesure où l'occurrence de réalisation du sinistre peut diminuer si les armateurs prennent toutes les mesures nécessaires pour la protection de leurs systèmes d'informations. C'est la raison pour laquelle les assureurs estiment que la réglementation joue un rôle fondamental pour la prise en charge du risque cyber.

En outre, les conséquences d'une cyberattaque peuvent impacter fortement la compagnie notamment avec la dégradation de l'image de la compagnie pouvant aboutir à une perte de compétitivité et au sabotage des systèmes informatiques du navire. Sur ce constat, il est primordial d'évaluer la vulnérabilité du navire aux attaques cyber. Et c'est sur cette base que des guides pratiques s'inscrivant dans la continuité des Directives

[42] https://www.ssi.gouv.fr/liste-produits-et-services-qualifies
[43] ISPS pour International ship and Port Facility Security, entré en vaguer le 1er juillet 2004.
[44] http://www.armateursdefrance.org/sites/default/files/decryptages/note_decryptage_-_gestion_des_cyber-risques_maritimes_21_10_19_vf.pdf

intérimaires de l'OMI sur la gestion des cyber-risques maritimes ont été rédigés avec le concours de l'ANSSI[45]:

- *Guide - Cyber sécurité- Evaluer et protéger le navire (Septembre 2016);*
- *Guide-Cyber sécurité- Renforcer la protection des systèmes industriels du navire (Janvier 2017);*
- *Guide des bonnes pratiques de sécurité informatique à bord des navires (Octobre 2016)*

Tous ces guides ont permis de sensibiliser sur la protection des navires. On peut donc noter une prise de conscience du risque cyber et une politique de sensibilisation des conséquences des cyberattaques.

Sous-section 2: La prise de conscience du risque cyber au niveau international

Au niveau international la prise de conscience n'a pas tardé, au vu des conséquences déjà désastreuses des quelques attaques cyber ayant touchées le secteur maritime. L'OMI s'est mis en premier rang pour aider les compagnies maritimes à se prémunir contre ce risque (A) ; s'en est suivi l'apport des associations internationales dans la réglementation (B).

A) Les efforts de l'OMI

Selon l'ONU, à l'heure actuelle, aucune réglementation contraignante au niveau international sur la cybersécurité dans le secteur maritime n'a été adoptée[46]. Toutefois des efforts ont été fournis par l'OMI avec l'élaboration du code ISPS (1) et du code ISM (2).

1- Les codes ISPS et ISM

Dans le secteur maritime, en ce qui concerne la sûreté, le code ISPS est l'outil réglementaire de référence. Entré en vigueur le 1er juillet 2004, il est composé de deux parties. Une partie dite « Obligatoire » et une partie dite « facultative ». Et c'est surtout la

[45] Documents disponibles sur le site du ministère de la transition écologique et solidaire (https://www.ecologique-solidaire.gouv.fr/surete-maritime)
[46] CNUCED, « Etude sur les transports maritimes », 2018, p93

partie « facultative qui traite des questions de cybersécurité. Cette seconde partie est obligatoire en Europe, suite au Règlement Européen 2004-725.

Il a pour objectif d' « *établir un cadre international faisant appel à la coopération entre les gouvernements contractants, les organismes publics, les administrations locales et les secteurs maritime et portuaire pour détecter les menaces contre la sûreté et prendre des mesures de sauvegarde contre les incidents de sûreté qui menacent les navires ou les installations portuaire utilisées dans le commerce international*[47]. »

Le code ISPS prévoit dans son article 8.3 de sa partie B que: « *l'évolution de la sûreté du navire devrait porter sur les […] systèmes de radio et de télécommunications, y compris les systèmes et réseaux informatiques* ». Ce qui veut dire que l'OMI à travers ce texte avait déjà recommandé aux compagnies maritimes, c'est à dire toute personne, telle que l'armateur gérant ou l'affréteur coque-nue, à laquelle l'affréteur a confié la responsabilité de l'exploitation du navire, d'anticiper sur les questions de cyber-risque.

Parallèlement, le code ISM[48], de manière générale, englobe les risques cyber émergents. Il oblige chaque compagnie à proposer des pratiques d'exploitation et un environnement de travail sans danger. Il impose également à évaluer tous les risques identifiés pour les navires, leur personnel et l'environnement, et à établir des mesures de précaution appropriées.

2- Les directives de l'OMI relatives à la cybersécurité

L'OMI, consciente de la menace et de l'impact que peut générer une attaque cyber, a élaboré plusieurs textes dans le but d'encadrer le risque cyber. En effet elle publie des directives[49] sur la gestion des risques cyber maritime. Ces directives ont pour objectif de fournir des recommandations et visent à protéger les transports maritimes contre les cyber risques. Elles prévoient que « *les directives contiennent des recommandations de haut niveau sur la gestion des cyber risques maritime afin de protéger le transport maritime*

[47] Code ISPS, Partie A, Objectifs 1.2.
[48] International Safety Management, entré en vigueur le 1er juillet 2002
[49] Circulaire MSC.1-FAL.1/Circ.3, 5 juillet 2017, OMI.

contre les cyber menaces et les vulnérabilité actuelles et émergentes. Les directives incluent également des éléments fonctionnels qui prennent en charge une gestion efficace des risques cyber[50] ». Ces directives recommandent aux armateurs de se conformer à un certain niveau de sécurité pour se prémunir des risques cyber.

Par ailleurs, le Comité de la Sécurité Maritime de l'OMI (MSC) a adopté le 16 juin 2017, une résolution sur la gestion des cyber risques maritimes dans le cadre des systèmes de gestion de la sécurité[51]. Ce comité reconnait dans l'alinéa 1er de la résolution qu': « *il est urgent de sensibiliser aux menaces et aux vulnérabilités en matière de cyber-risques afin de renforcer la sécurité et la sûreté des transports maritimes pour qu'ils aient une résilience opérationnelle face aux cyber-risques* ». Il encourage les administrations à s'assurer que les cyber-risques sont convenablement incorporés dans les systèmes de gestion de la sécurité. Cette recommandation doit être appliquée au plus tard à la date de la première vérification annuelle du document de conformité délivré à la compagnie après le 1er janvier 2022.

En plus, dans *l'Étude sur les transports maritimes 2018*, la CNUCED souligne que l'OMI reconnait la nécessite d'intégrer les technologies nouvelles et avancées dans le cadre réglementaire du transport maritime en trouvant un juste équilibre entre les avantages découlant des technologies nouvelles et avancées « et les préoccupations liées à la sécurité et la sûreté, les conséquences pour l'environnement et la facilitation du commerce international, les éventuels coûts pour le secteur et, enfin, les répercussions sur le personnel à bord et à terre[52] »

A l'heure actuelle, les travaux se poursuivent au niveau du MSC pour perfectionner les dispositions issues des textes de 2017. Notons que les Etats-Unis ainsi que certaines organisations représentatives du shipping ont élaboré des propositions en faveur d'une

[50] Version originale : « The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management ».
[51] Résolution MSC.428(98)
[52] IMO, Strategic plan for the Organization for the six-year period 2018 to 2023. A.1110 (30), London. 8 December 2017

application uniforme des directives sur la gestion des cyber-risques maritimes et d'une harmonisation des exigences du code ISM et du code ISPS[53].

Les efforts de l'OMI dans la réglementation ne paraissaient pas suffisants pour encadrer, de manière générale la gestion des cyber-risques maritimes. Il fallait donc passer du bon vouloir personnel aux efforts collectifs. Les travaux de l'OMI sont complétés par ceux des associations maritimes internationales qui ont apporté leur soutien à travers l'International Chamber of Shipping (ICS) et le Baltic and International Maritime Council (BIMCO).

B) L'apport des associations maritimes internationales dans la réglementation

1) Baltic and International Maritime Council (BIMCO)

Le monde maritime a beaucoup fait pour embrasser le monde digital ces dernières années. Cette évolution numérique se justifie par une politique économique de coûts et d'efficacité. Mais au-delà des nombreux avantages de l'internet, il existe quelques écueils potentiels à surmonter.

La cybersécurité dans le domaine maritime est devenue un sujet brûlant au cours des 3 dernières années. L'incident cyber de *Notpetya* qui a touché Maersk en 2017 et d'autres incidents cyber similaires plus récents impliquant de grands ports ont marqué le secteur maritime. Pourtant beaucoup d'acteurs du secteur se sentaient à l'abri des menaces posées par les cybercriminels. Mais ces attaques répétitives ont démontré qu'aucune entreprise n'est en sécurité, car les attaques cyber peuvent être directement ciblées ou simplement faire partie d'un effet en cascade chez un fournisseur ou une société tierce. Ce qui veut dire que toute la chaîne logistique est exposée aux cyber-risques et la réaction devient alors urgent. C'est pourquoi les associations maritimistes ont pris les devants pour adapter une culture cyber dans la gestion de la sécurité des systèmes.

Dans un manuel publié en 2019 intitulé « Cyber Security Workbook for Board Ship Use[54] », BIMCO, en association avec ISC démontrent que le risque cyber est un réel

[53] Voir les travaux du Comté de la Sécurité maritime lors de la 101ème session.

problème dans le milieu maritime qu'il est urgent de résoudre. Ce manuel est aligné sur les lignes directrices produites par la résolution MSC.428(98) de l'OMI.

Le document a d'abord élaboré une identification des risques, menaces, et vecteurs d'attaques les plus courants, des logiciels malveillants aux clés USB de l'équipage et à l'ingénierie sociale; avant d'approfondir la protection et la prévention. Selon eux « *il est impossible d'être complètement cybersécurisé, même si une gestion efficace de la cybersécurité peut réduire la probabilité et la gravité d'un incident. La création d'une culture et d'une conscience cybernétique, centrée sur les mesures de protection, de prévention et de formation est cruciale*[55] ». Cela montre que le secteur maritime doit s'habituer à prendre plus de responsabilité dans la gestion du risque cyber. Cette prise de responsabilité ne peut cependant être pertinente que si la règlementation et les normes édictées sont respectées.

En plus, ils demandent aux compagnies maritimes de disposer de réponses efficaces, leur permettant de minimiser les dommages et de remettre les systèmes en état de fonctionnement normal dès que possible. Ce qui nécessite l'élaboration d'un plan d'intervention en cas d'incident cyber[56]. Ceci en essayant d'abord d'isoler ou d'arrêter le système affecté et ensuite déclencher quatre étapes de récupération. Ce plan d'intervention permettrait à la compagnie victime d'attaque cyber d'informer les autorités compétentes mais surtout permettre aux assureurs d'établir la gestion de sinistre.

2) Les recommandations des associations sectorielles

Dans de nombreuses recommandations, le secteur du transport maritime a fourni des orientations pratiques sur la gestion des cyber-risques par les compagnies et prévoit des données pratiques pour le marché de l'assurance. Dans une étude antérieure[57] BIMCO, en association avec d'autres organismes du secteur, avaient déjà souligné que la gestion des

[54] BIMCO, Cyber Security Workbook for Board Ship Use, Edition 2019.
[55] Version originale: « It is impossible to be completely cyber secure, although effective cyber security management can lessen the likelihood and severity of an incident. Creating a culture of cyber awareness, centred around protective and preventative measures and training is crucial », *Ibid, page 9.*
[56] *Ibid., p39.*
[57] BIMCO, CLIA,ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI : « The guidelines on cybersecurity on board ships, version 2.0, 2017.

cyber-risques nécessite d' « *identifier les rôles et responsables des utilisateurs, des personnels clefs et des cadres à terre comme en mer; recenser les systèmes, les actifs, les données et les capacités, qui pourraient menacer l'exploitation et la sécurité des navires en cas de perturbation; mettre en place des mesures techniques pour protéger contre un cyber incident et assurer la continuité de l'exploitation. Il peut s'agir de la configuration des réseaux, du contrôle des accès aux réseaux et aux systèmes, des communications et des limites de confiance et de l'utilisation de logiciels de protection et de détection; mettre en œuvre des activités et des plans (mesures procédurales de protection) pour assurer la résilience face aux cyber incidents. Cela peut concerner la formation et la sensibilisation, la maintenance logicielle, l'accès à distance ou local, les privilèges d'accès, l'utilisation d'appareils multimédias amovibles et la mise au rebut de matériels; et mettre en œuvre des activités visant à se préparer aux cyber incidents et à réagir lorsqu'ils surviennent*. »

L'application à la lettre de tous ces éléments permettrait aux compagnies maritimes de mieux se prémunir contre les attaques cyber et probablement de rassurer les assureurs à s'investir davantage dans les risques cyber.

La réglementation est un point non négligeable dans la prise en charge d'un risque par les assureurs. En effet, les assureurs ont besoin de connaître la capacité de gestion des cyber-risques des assurés. De manière générale, « *les normes sont des exigences et des points de contrôle permettant aux entreprises de décliner les exigences réglementaires et les exigences de sécurité, tout en rassurant les interlocuteurs externes et la direction*[58] *.* » A cela s'ajoute la réduction de l'aléa moral issu d'un potentiel « comportement particulier » de l'assuré qui peut créer un blocage entre l'intérêt de l'assuré et de l'assureur. Le respect des normes par les compagnies maritime surtout pour les risques cyber réduirait considérablement les chances d'occurrence du sinistre et pousserait probablement les assureurs à prendre plus de risques.

La réglementation permettrait dans une certaine mesure d'avoir une attitude pro-active face aux cyber-risques et éventuellement réduire leur impact. En plus, les compagnies maritimes doivent mettre en place une commission d'audit des risques de

[58] Voir compte rendu du groupe de travail cyber risque Institut des Actuaires sur le thème « Emergence du besoin en cyber assurance »Animé par Carole Mendy, 2017.

systèmes d'information au sein de l'entreprise, permettant ainsi d'évaluer leur niveau de sécurité et de prévenir la sélection adverse ou anti-sélection de l'assureur. Mais en réalité la quantification du risque cyber est d'une complexité, qui n'encourage pas sa prise en charge par les assureurs.

CHAPITRE 2- LA QUANTIFICATION COMPLEXE DU RISQUE CYBER

A l'heure actuelle peu de compagnies d'assurance s'engagent dans la couverture du risque cyber. La raison de cette réticence s'explique par la quantification complexe du risque, à cause de sa méconnaissance technique (Section 1) ; mais surtout par le fait que c'est un risque évolutif qui change au rythme de la technologique (Section 2).

SECTION 1- LA MÉCONNAISSANCE TECHNIQUE DU RISQUE CYBER

La méconnaissance du risque cyber est due à une absence de statistiques sinistres **(Sous-section 1**) du côté des assureurs et réassureurs. Ce manque de données ne facilite pas leur accompagnement des compagnies maritime dans la prévention et la protection contre le risque cyber (Sous-section 2).

Sous-section 1: L'absence de statistiques sinistres

Le développement industriel depuis le milieu du 19ème siècle a généré de nouveaux risques de plus en plus graves. Ceci nécessite de la part des assureurs l'augmentation de leurs capacités surtout pour la couverture des risques de grande ampleur comme les risques cyber.

Les assureurs ont habituellement tendance à couvrir les risques traditionnels mais l'évolution de la technologie a accéléré l'apparition de nouveaux risques. Le risque cyber est l'un des risques les plus complexes pour les assureurs tant dans le calcul de sa probabilité(B), que dans ses statistiques permettant une meilleure modélisation(A).

A- Les manquements dans la modélisation du risque cyber

1) Le problème de la tarification

Depuis plusieurs années, on assiste à une recrudescence des attaques cyber dans le monde maritime. Ces attaques causent dans la plupart des cas des dommages aux infrastructures mais aussi aux biens. Minimisées ou mal connues des acteurs maritimes, ces

attaques ont causé plusieurs milliards de dollars de dommages au monde maritime. L'espace maritime est occupé par de grandes sociétés qui investissent dans des navires dont le montant peut dépasser les 150 millions de dollar. Donc un seul risque cyber peut avoir des conséquences désastreuses sur l'économie de la société. Ainsi

Les assureurs ont besoin de données, leur permettant d'avoir une vision assez claire sur les risques à prendre. Mais on constate, à ce jour, un manque considérable de base de données exploitable sur le marché du risque cyber. Cela complique davantage la tarification du risque avec une multitude d'incertitudes autour des coûts qu'il peut engendrer. Cette situation rend les assureurs plus conservateurs lors de la tarification des contrats, et les incite à appliquer des limites de garanties.

Selon une étude de Marsh, en 2015[59], le coût médian de couverture pour un contrat type cyber est trois à six fois plus élevé que pour des contrats de types RC ou dommages (**Voir annexe2).**

En plus, le rapport nous apprend qu'il y a une variabilité des tarifs moindres pour les contrats type cyber et cela démontre la difficulté à différencier deux risques. À l'heure actuelle, plusieurs critères permettent de différencier les risques:

- Le secteur d'activité;
- Des indicateurs clés tels que le chiffre d'affaires;
- La capacité à traiter, stocker et sécuriser des données à caractère personnel;
- Le niveau de sécurité des systèmes d'information et de conformité aux normes.

Tous ces éléments permettent aux assureurs de faire la différenciation.

Selon les chercheurs « *les ajustements tarifaires peuvent se faire par le biais de franchise, de limites et de chargement de sécurité*[60] ». Dès lors, le niveau de prime au regard de l'appréciation de la couverture est souvent cité comme l'un des obstacles importants à la souscription d'assurance cyber[61]. Cela se justifie par le fait que de nombreux assureurs fixent des limites inférieures aux niveaux recherchés par leurs clients. Ce qui fait que le maximum est de 500 millions de dollars, bien que la plupart des grandes

[59] UK Cyber security : The Role of Insurance in Managing and Mitigating the Risk – Marsh 2015
[60] Club des juristes : « Assurer le risque cyber », janvier 2018, p52.
[61] PwC, Insurance 2020 & beyond, Reaping the dividends of cyber resilience, 2015, p. 10.

entreprises aient du mal à obtenir plus de 300 millions de dollars[62]. Mais compte tenu des coûts élevés de la couverture, des limites imposées, des conditions d'attachement strictes et les conditions et restrictions quant à la possibilité pour les assurés de faire une réclamation, de nombreux clients se demandent si leur police cyber offre une valeur réelle.

Il y a aussi le problème de la modélisation du risque cyber. Cette modélisation des capacités de gestion des cyber risques « *mesure précisément l'écart entre les pratiques d'une société et ce qu'on peut considérer comme les meilleures pratiques*[63] ». Dans un rapport publié par Hiscox, on apprend que seul 10% des entreprises dans tous les secteurs confondus ont obtenu la mention « experts » dans la capacité de gestion des cyber-risques. Plus de 74% n'ont obtenu la mention « expert » dans aucun des domaines (Stratégie, contrôle, ressources, technologie et procédure) et 16% sont intermédiaires, c'est à dire celles ayant satisfait partiellement aux exigences de la modélisation. Il apparait donc que la majeure partie des entreprises ne sont pas bien préparé face à la menace.

Toutefois, avec la nouvelle réglementation, on peut espérer que les choses vont progressivement évoluer et le niveau des primes peut être réduit. Cependant le marché du cyber risque est loin d'être maitrisé en raison de l'asymétrie d'information des acteurs, du niveau de sécurité interdépendants des navires et des faibles incitations à l'investissement. Il y a un manque d'appétit remarquable des assureurs sur le marché du cyber-risque et cela est dû à la complexité tant dans sa définition que dans sa quantification.

2) L'asymétrie d'informations

L'incapacité du marché de risque cyber à devenir un véritable marché concurrentiel est due à un certain nombre de problèmes non résolus jusque-là ainsi qu'à des considérations pratiques[64]. Les plus importants d'entre eux sont l'asymétrie entre les

[62] Financial Times, 18 février 2015.
[63] Rapport Hiscox sur la gestion des cyber-risques, 2019, p8.
[64] Ranjan Pal, Cyber-Insurance for Cyber-Security. A Solution to the Information Asymmetry Problem, University of southern California, 2012

assureurs et les assurés[65], et la nature interdépendante et corrélée du cyber-risque[66]. L'asymétrie d'information à un effet significatif sur la plupart des environnements d'assurances et se compose de trois éléments: d'abord l'incapacité de l'assureur de distinguer les utilisateurs de types différents. C'est à dire la capacité d'effectuer une sélective adverse ou encore « anti sélection ». Ensuite un processus qui consiste à classer les assurés par groupe afin de déterminer les primes. Et enfin des utilisateurs ayant un comportement imprudent de nature à augmenter les chances d'occurrence du sinistre ; ceci correspond à l'aléa moral. Cependant, beaucoup d'entreprises ne veulent pas dévoiler leur vulnérabilité par peur de nuire à leur réputation. Cela donne une asymétrie de l'information: l'assureur connait beaucoup moins bien les risques comme son assuré.

Dans le cas du cyber-risque cette asymétrie est parfois trop importante entre assureurs et assurés. C'est le cas par exemple d'entreprises qui cherchent à assurer certains de leurs actifs sur la nature et la gestion sur lesquelles elles doivent maintenir le secret. L'assureur n'est alors pas en mesure de se prémunir du phénomène d'« anti-sélection ». Il arrive que, l'assureur ne dispose pas suffisamment de données lui permettant d'estimer son exposition à un certain risque et ne souhaite pas porter individuellement des contrats en indemnisant les conséquences. Ceci est dû parfois à la réticence de l'assuré de partager certaines informations jugées confidentielles. Ce qui ne facilite pas la quantification du risque cyber, car les assureurs doivent avoir une « *fine connaissance de l'entreprise cliente pour comprendre les menaces auxquelles elle doit faire face*[67]. » Mais à ce stade du développement du marché de l'assurance cyber, l'asymétrie d'informations est très importante et n'encourage pas l'évolution future du marché. Elle ne permet pas aux assureurs d'établir un calcul d'une prime adaptée aux spécificités du profit de l'assuré et ainsi généraliser des phénomènes d'anti-sélection. Par conséquent, deux types de cibles se présentent. Il y a ceux qui sont déjà victime d'attaque et qui veulent se protéger d'une éventuelle prochaine attaque en transférant le risque aux assureurs ; et ceux qui ne

[65]T.Bandyopadhyay, V.S. Mookerjee, R.C. Rao, Why IT managers don't go for cyber-insurance products,Communications of the ACM 52
[66] R.Bohme, G.Schwartz, Modeling cyber-insurance:Towards a unifying framework, in:WEIS,2010.
[67] Club des Juristes, Assurer le risque cyber, janvier 2018, p32

s'estiment pas le plus à risque et ne s'assurent. Cette division des potentiels clients déséquilibre la porte de risque des assureurs.

Nous venons de démontrer que la question de l'assurabilité du risque cyber a toujours animé les débats, mais plutôt que de nous prononcer ou de chercher à se positionner sur le développement ou l'échec du marché, nous optons de faire preuve de pragmatisme et aller dans le concret en réfléchissant aux moyens que l'assurance, au sens large, pourrait mettre en place pour accompagner les acteurs maritimes pour faire face aux risque cyber.

B) La problématique de l'outil de calcul de probabilité du risque cyber

1) Les contraintes matérielles sur différents niveaux

L'assurance est subordonnée à la connaissance du risque qui dépend d'événements aléatoires nécessitant la construction d'outils de calcul. Très souvent, la couverture d'un risque peut être compliquée lorsqu'il y a un manque d'informations statistiques sur le risque en question. Les assureurs ont besoin d'un outil leur permettant de mesurer la probabilité du risque. Le principal outil qui est le calcul des probabilités est né en France au 17ème siècle. A cette époque fut réalisé, pour la première fois, un outil permettant de réaliser des calculs actuariels. C'est à dire de mesurer les paramètres des contrats d'assurances. Et aujourd'hui, grâce à la qualité des estimations sur les probabilités du risque, les assureurs peuvent connaitre l'activité et sa rentabilité.

Même si cela semble simple pour les risques traditionnels, il ne l'est guère pour le risque cyber, qui pendant longtemps a été minimisé par les acteurs économiques.

Pour être assurable, les pertes associées à un risque donné doivent être estimées et modélisées grâce à l'analyse de séries historiques d'événements passés[68]. Cela veut dire que l'estimation du risque dans sa globalité reste fondamentale pour sa prise en charge. Dans le cas du cyber risque, les assureurs ne disposent pas d'assez d'informations sur la fréquence et la gravité des attaques cyber. La nouveauté de ce risque fait que les calculs actuariels se basent sur des séries historiques étroites. Ce qui ne donne pas une large marge

[68] Club des Juristes, Assurer le risque cyber, p.28-29

de manœuvre aux assureurs dans le calcul de la probabilité du risque pour plusieurs raisons:

- D'une part, le risque cyber est un risque récent, dont les conséquences ont commencé à se sentir dans les années 90. Le début de l'année 1990 est ainsi concomitant à l'émergence d'une sous-culture criminelle cybernétique[69]. La première cyberattaque de grande ampleur est recensée il y a une douzaine d'année, avec l'attaque contre le centre informatique estonien. Dans le monde maritime, l'attaque contre Maersk en 2017 reste la plus importante avec une perte évaluée à plus de 300 millions de dollars. Il est clair que l'historique du risque cyber est très récent contrairement à celui développé sur les autres risques. En plus la politique de collecte de données de sinistralité est engagée très récemment après les premières apparitions.

- D'autre part, il s'agit d'un risque extrêmement évolutif, qui devient de plus en plus difficile à cerner. Ce caractère évolutif du risque se mesure sur trois aspects: la digitalisation des navires, qui devient de plus en plus récurrente dans l'espace maritime, l'augmentation des vagues de délinquance avec l'utilisation de moyens techniques et matériels plus importante et enfin l'évolution de la réglementation. Si pour les acteurs du monde maritime, l'objectif est de trouver des moyens de plus en plus sophistiqués pour la prévention et la protection des S.I des navires pour éviter toute intrusion ; les attaquants, quant à eux, ont pour objectif de détourner ces garde-fous pour pénétrer les S.I des compagnies maritimes en mer ou à terre.

Il semble donc primordial, pour les assureurs, de développer un langage commun, à partir duquel, s'établissent une définition et une classification des différents vecteurs du risque, ses conséquences et ses caractéristiques techniques. Ce qui veut dire que : « *sans l'établissement d'un vocabulaire commun, aucun partage d'information et d'historique entre assureurs ne sera possible car chacun a développé des conceptions propres du risque incompatibles entre elles*[70]. » Il est donc fondamental, d'établir une plateforme publique de collecte des données, même si la question de la confidentialité peut se poser.

[69] Philippe Baumard, La cybercriminalité comportementale: Historique et régulation, Vol 3, Octobre 2014, p44

[70] Gaspard FEREY Nicolas GROROD Simon LEGUIL, L'assurance des risques cyber, Mines ParisTech, 2017, p56

2) Les contraintes techniques

Il existe deux contraintes techniques sur les données statistiques disponibles sur les incidents cyber. D'une part il n'y pas de méthodologie standardisée pour inventorier de manière homogène les sinistres cyber et leur impact à l'échelle nationale et internationale. Cela faciliterait largement la connaissance du risque cyber par le biais des bases de données disponibles. Cependant nous nous sommes posé un certain nombre de questions à savoir qui gère la collecte d'informations relatives aux incidents cyber? Sur quel fondement doit-il se baser? Quels types d'incidents cyber méritent d'être comptabilisés dans la base de données? Comment déterminer la gravité de l'incident en fonction des conséquences dommageables? Comment définir le seuil de gravité? Toutes ces questions ne trouvent pas de réponses partagées, prouvant ainsi la complexité de la mesurabilité du risque.

D'autre part, il existe une multitude d'organismes privés qui ont tendance à publier des statistiques sur les attaques cyber. Seulement, aucun organisme, à ce jour, en France, n'est habilité à collecter et anonymiser les sinsitres cyber à l'échelle nationale afin de produire des statistiques fiables qui pourrait être partagées avec tous les acteurs du marché. Cette absence d'organisme unique marque la difficulté pour les assureurs de maitriser le cyber-risque dans sa globalité.

En outre, les données disponibles permettent seulement d'évaluer la fréquence des attaques et le volume des données compromises, sans pour autant fournir des détails sur les impacts financiers pour les entreprises.

La probabilité de succès des attaques cyber repose sur le degré de maturité de la cible et la nature de l'attaquant, mais avec une dissymétrie de moyens plutôt en faveur de l'agresseur. Également, les risques cyber se distribuent souvent par vagues (vol de données pour détourner l'itinéraire du navire, rançonnage etc.) en fonction de la technologie (vulnérabilité d'un logiciel, corrélation du risque etc.) ou de l'environnement géopolitique. Notons aussi que certaines grandes entreprises génèrent un tropisme avéré des « *hacktivistes* ».

Tous ces éléments méritent d'être pris en compte. Semblablement au risque politique ou au risque de guerre, dont ils héritent en partie, il pourra s'avérer que sous

certaines conditions, les facteurs de menace ou de vulnérabilité feront perdre au risque cyber son caractère aléatoire[71].

L'absence de base de données fiables prive les assureurs d'un outil essentiel pour modéliser les risques cyber et l'ensemble des acteurs économiques d'une source d'informations qui contribuerait à une prise de conscience accrue du risque cyber.

Sous-section 2: Les difficultés en matière de prévention et de protection

Nous venons de démontrer que le risque cyber dans le monde maritime est un risque méconnu des assureurs ou du moins mal maitrisé. Pourtant les complications ne se limitent pas là, car il y a un manque considérable de ressources humaines spécialisées à bord des navires (B) pouvant intervenir en cas d'attaque pour réduire les conséquences. Mais les compagnies maritimes doivent au préalable renforcer leur niveau de sécurité pour faciliter leur accompagnement par les assureurs (A).

A) : Le problème de la sécurisation des navires

S'il y a au moins un facteur qui empêchent les assureurs de stimuler leur appétit sur le risque cyber, c'est bien le niveau de cyber maturité des compagnies maritime.

1) Le niveau de cyber maturité des compagnies maritimes:

De par leur niveau de protection

Le navire est le premier instrument de la navigation. Sa protection doit être au centre des préoccupations des armateurs. La protection du navire et de ses équipements se définit à travers le matériel mais également les systèmes informatiques. C'est seulement si ses éléments factuels sont assurés que l'on peut parler de maturité.

Le voyage maritime est une longue aventure qui demande un contrôle permanent du navire mais aussi des biens transportés. C'est la raison pour laquelle, les armateurs soucieux d'innombrables risques préfèrent transférer les risques aux assureurs.

Depuis plusieurs années, on note une recrudescence des risques cyber qui parfois, est lié à la vulnérabilité des mesures de sécurité prises par les armateurs. La sécurisation

[71] Sébastien HEON et Didier PARSOIRE, « la couverture du cyber-risque », extrait de la Revue d'Economie Financière, n° 126, P7.

des navires est au cœur de cette problématique. Dans une note stratégique[72] du CEIS publiée en janvier 2017, trois experts ont démontré que : « *la sécurisation des navires nécessite en premier lieu la sécurisation by design des architectures (cloisonnement et protection de chaque sous réseau ainsi constitué, systèmes de protection périphérique (pare-feu, anti-virus), système d'authentification et de gestion des droits d'accès, systèmes de journalisation, etc.)* Pour eux, la protection des navires doit d'abord commencer par la sécurisation des S.I qui sont une porte d'entrée pour les cybercriminels. Les armateurs et équipages doivent avoir un œil permanent sur les systèmes informatiques. C'est ce qu'on appelle le maintien en condition de sécurité[73] (MCS) des équipements numériques embarqués qui est quasi-absent dans l'exploitation des navires. C'est un problème fondamental que les assureurs prennent en compte dans la prise en charge du risque cyber. A cet effet l'assuré doit prendre toutes les mesures nécessaires afin d'éviter la réalisation du risque. La diligence et la prudence doivent être de rigueur mais on constate qu'il n'existe peu d'experts cyber dans les navires pouvant agir en cas d'attaque.

De par leur niveau de prévention

Par ailleurs cette sécurisation ne se limite pas seulement à la protection des S.I, la prévention permet également d'anticiper les risques qu'encours le navire. C'est pourquoi Xavier De Korsak[74] expliquait que : « *notre conviction est que le principal levier de progression pour devenir une entreprise cyber résiliente réside dans la prévention et le diagnostic nécessaires à une démarche d'amélioration continue*[75] . » L'idée est de permettre aux entreprises d'évaluer leur niveau de maturité face aux risques de sécurité informatique. Mais aussi de connaitre leur niveau d'exposition aux risques d'une cyberattaque de type phishing/ransomware ou de limiter leur exposition au risque d'erreurs humain par la sensibilisation des collaborateurs ; et enfin d'appréhender les sujets de cybersécurité à étudier en premier. Cela permettrait aux assureurs de mieux comprendre le risque ainsi que l'état de prévention et de protection des navires face au risque cyber. Nous

[72] CEIS, Note stratégique, Cybersécurité dans le milieu maritime: défis et pistes de solutions, William Pauquet, Josselin Bercy et Michel Benedittini, janvier 2017, p32.
[73] *id*
[74] Directeur associé et cofondateur de Harmonie Technologie, spécialisée dans la cybersécurité. https://www.solutions-numeriques.com/securite/r/?id=18434&type=1

aurons l'occasion d'insister sur la prévention quand nous évoquerons les défis que les assureurs doivent relever dans la partie deux.

B) Le manque de ressources humaines spécialisées en cyber-risque

Ici il sera question d'étudier, le manque ou l'absence d'experts spécialisés en cyber risque. En effet ce manque de ressources humaines spécialisés en cyber risques n'est pas problématique en soi. Les armateurs peuvent mettre en place des mesures techniques comme des SIEM (Security Information Event Management System) et des SOC (Security Opération Center) à terre[76] permettant de contrôler le navire et de prendre les mesures nécessaires en cas d'attaque. Mais la mise en place de ce type d'organe peut être difficile en raison de sa complexité mais aussi de son coût. Le SEIM par exemple permet de contrôler des applications, des comportements d'utilisateurs et des accès aux données dans le but de collecter, agréger, normaliser, corréler et analyser les données fournies par les machines et systèmes d'exploitation à la suite d'événements majeurs. C'est un projet qui permettrait sans doute aux armateurs de mieux lutter contre le risque cyber. Toutefois, cela n'est pas si simple comme il le parait pour deux raisons: d'une part la plupart se focalise plus sur la compétitivité et la rapidité que sur les questions de prévention contre les risques informatiques; d'autre part les compagnies maritimes ne sont pas de la même taille. En effet, certaines entreprises ont une force de frappe suffisante leur permettant de mettre en place ce type d'organe, des processus de management du risque et des compétences techniques de prévention et de gestion de crises. D'autres, par contre seront obligées de se lier sur un écosystème de prestataires spécialisés.

On est face à une variété de profils pour un même risque et donc une solution unique ne suffira pas pour la simple et bonne raison qu'elle ne pourra pas prendre en compte tous les paramètres des deux profils susmentionnés. Donc, il faut « *mettre en avant une grille d'analyse basée sur la taille de l'entreprise et son secteur d'activité*[77]. » C'est à

[76] CEIS, Note stratégique, Cybersécurité dans le milieu maritime: défis et pistes de solutions, William Pauquet, Josselin Bercy et Michel Benedittini, janvier 2017, p33.
[77] Gaspard FEREY, Nicolas GROROD, Somin LEGUIL, L'assurance des risques cyber, comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive?, 2017, p38

dire faire une analyse sectorielle des entreprises afin de connaître la spécificité nécessaire au traitement du risque dans chaque entreprise.

Le manque est flagrant dans le secteur maritime où l'on note une absence quasi total d'experts à bord ou à terre pouvant intervenir en cas d'attaque cyber. Toutefois la solution du SIEM pourrait être difficile à appliquer car, exceptés les acteurs essentiels du commerce maritime mondial ayant une capacité supérieure à 1 million d'EVP (Equivalent Vingt Pieds) (Maersk, CMA CGM, MSC), tous les autres ont plus ou moins la même capacité (Hapag-Lloyd, Evergreen Line, Cosco etc). Donc la mise en place d'un système de contrôle peut sembler très futuriste pour les « petites » compagnies pour des raisons financières.

SECTION 2- L'EVOLUTION DU RISQUE CYBER AU RYTHME DES PROGRES TECHNOLOGIQUES DES SYSTEMES INFORMATIQUES

Depuis quelques on assiste à une migration remarquable du secteur maritime vers le numérique. Cela s'explique par le besoin de rapidité dans les transactions mais aussi pour des raisons de compétitivité. Mais cette digitalisation, malgré ses nombreux avantages tant dans le contrôle et la traçabilité, rend les navires cyberdépendants (**Sous-section 2**) et peut être source de vulnérabilité des systèmes d'information des compagnies (**sous-section 1**).

Sous-section 1: La digitalisation des navires: source de vulnérabilité des systèmes d'information.

La transformation numérique du monde maritime s'est accélérée dans la dernière décennie. Ce changement a amené de nouveaux risques auxquels le secteur maritime doit faire face. L'apparition de nouveaux risques dus à la révolution digitale des navires (A), s'accentuera probablement avec l'avènement des navires autonomes (B).

A) La révolution digitale des navires classiques

Le transport maritime consiste au déplacement d'une marchandise d'un point A à un point B. C'est un mode de transport qui représente 90% du commerce mondiale. Donc l'usage de moyen de transport efficace et fiable est nécessaire. Le navire a toujours été au centre du monde maritime; son évolution au fil des années marque le besoin de transporter

le plus de marchandises. Entre 1969 et 2019, on est passé de 1572 EVP à 23756 EVP[78]. Un tel gigantisme nécessite une sécurité technologique efficace pour son contrôle et sa traçabilité. C'est justement ce que permettent les nouvelles technologies. En effet, depuis plusieurs années, on assiste à une digitalisation des navires, qui modifie comme ailleurs bien des choses. La recherche de la productivité et de la compétitivité dans un contexte de concurrence et de marché dégradé oblige à l'innovation. Mais cette révolution a été un élément accélérateur du risque cyber (1)

1) Un élément accélérateur du risque cyber

Les progrès techniques et technologiques ont toujours révolutionné les activités humaines et le monde maritime n'échappe pas à cette règle. Ce progrès technologique facilite la transparence, la rapidité et l'instantanéité. C'est à cet effet que Rodolphe SAADE disait : « *la digitalisation de notre économie va en effet révolutionner notre activité*. » Le navire est devenu un objet traçable avec l'apport des technologies satellitaires. Cette traçabilité (AIS) a vu le jour vers les années 1990 mais il a fallu attendre la convention de SOLAS pour la généraliser. *L'Automatic Identication System* (AIS) est un instrument qui permet de localiser les navires au-delà des radars. Ce qui est un progrès important dans le secteur et qui permet la mise en place des VTS (Vessel Traffic Services).

La sécurité maritime est renforcée avec cette réalité instantanée de la navigation[79]. Beaucoup d'autres outils comme le VTMIS (Vessel Traffic Management and Information Services) ou l'ECDIS (Electronic Chart Display and information System) ont permis de mieux sécuriser et contrôler le navire, avec la programmation des escales des navires en liaison avec la capitainerie, les agents maritimes, les services portuaires. Non seulement le navire est physiquement contrôlé grâce à la technologie, mais il l'est aussi dans les bases de données. Le ***tracing*** du navire n'est qu'un apport des technologies d'information. La digitalisation des biens, des machines et appareils de bord, représente des centaines d'informations qui sont produites et utilisables par le bord, mais aussi par l'armateur. L'un des outils informatiques de performance et d'optimisation pour le bord mais aussi pour les

[78] https://insolentiae.com/wp-content/uploads/Le-plus-gros-porte-conteneurs-au-monde.
[79] ISEMAR, 20 ans d'apports des technologies aux industries maritimes, note de synthèse, n°191, juin 2017,p2

acteurs à terre, est le ***monitoring.*** Cet outil permet d'évaluer en temps réel des systèmes physiques par des capteurs et censeurs transmettant des informations.

Certes cette révolution technologique est importante et nécessaire dans un secteur qui représente plus de 90% du commerce mondiale, mais elle n'est pas sans risque car le navire est de plus en plus exposé aux risques technologiques.

La digitalisation est l'un des facteurs du cyber-risque. En effet, il n'est nul besoin d'être un hacker pour connaitre le positionnement instantané d'un navire, son identité ou son statut. Cela pourrait être un moyen pour les cyber-pirates d'introduire dans les systèmes informatiques des navires pour détourner ou contourner le système.

Cette augmentation du risque cyber avec la digitalisation n'encourage pas les assureurs dans la prise en charge d'un tel risque car l'occurrence de réalisation du risque devient de plus en plus élevée avec des outils de navigation ou de contrôle parfois méconnus par les assureurs. Comme l'expliquait Sébastien LOOTGIETER : « *Nous sommes face à une industrie de plus en plus informatisée et connectée, mais il y a un manque de conscience de la réalité du cyber-risque chez les opérateurs maritim*es[80]. » Cela veut dire qu'il y a une méconnaissance accrue du risque cyber dans le monde maritime. Et contrairement au transport terrestre ou aérien qui a très vite pris en charge ce risque, le transport maritime est largement en retard dans sa prise de conscience. C'est ce qu'on peut lire dans une étude menée par le KPMG, en date du 24 mai 2014: « *la cybersécurité à bord des navires de commerces et dans les principaux ports avait 10 à 20 ans de retard par rapport aux systèmes des ordinateurs terrestres, laissant ainsi une porte ouverte à une échelle de menaces de plus en plus importantes*[81]. »

B) Les navires autonomes

Il est vrai qu'il est peut-être prématuré de poser le débat sur l'assurance des risques cyber sur les navires autonomes en raison de sa complexité mais aussi de sa définition.

[80] Sébastien LOOTGIETER, les risques cybernétiques dans le domaine des transports, Lamy, DMF 775, décembre 2015,p2

[81] Version originale: « Cyber security on board merchant vessels and at major ports is 10 to 20 years behind the curve compared with office-based computer systems, leaving them wide open to an ever-increasing range of threats, according to the director of information protection at advisory firm KPMG », Lloyd's List, 6 mai 2014

Néanmoins dans une vision futuriste de la navigation[82], il serait pertinent de soulever la question de manière anticipée afin d'apporter des perspectives lorsque la question se posera plus tard de manière concrète.

La vision très futuriste des navires autonomes est apparue il y a quelques années. L'idée peut être discutable, mais on en est à l'évidence qu'à ses balbutiements. L'objectif est de supprimer tout humain du navire pour en faire un outil de transport autonome et contrôlé à distance[83]. Cela peut être motivé par l'envie de réduire les risques liés au facteur humain dans le monde maritime. Sans pour autant trop entrer dans les aspects techniques de ce projet « futuriste », il semble inévitable de soulever la question de sa vulnérabilité, car même avec équipage le navire demeure vulnérable. Reste à savoir s'ils sont des espaces de risque cyber flagrant (1) ou un espace d'inassurabilité du risque cyber (2) en raison des coûts.

1) Un espace de risque cyber flagrante

La question de l'assurabilité des navires autonomes semble pour certains assureurs prématuré car selon le groupe Chubb[84] : « *tous les facteurs permettant d'examiner les risques et d'assurer les navires sans équipage ne sont pas réunis, car il y a d'énormes problèmes culturels.* » Cela veut dire que l'assurance des navires autonomes n'est pas encore à sa maturité. On peut dire qu'il y a une certaine méfiance des assureurs en raison de l'exposition des navires aux risques en l'occurrence les risques cyber.

La question de l'assurance des risques cyber dans les navires classiques est déjà assez complexe, mais le risque cyber est un risque universel qui touche tous les secteurs économiques et tous les infrastructures, à plus forte raison, les navires autonomes qui sans équipages, naviguent dans les espaces les plus hostiles. Cela nous pousse même à penser que le risque cyber peut être plus présent dans les navires autonomes que dans les autres.

[82] Lasmoles Olivier, Cybersécurité et navires sans équipages, DMF n°817, Octobre 2019, p772
[83] ISEMAR, 20 ans d'apports des technologies aux industries maritimes, note de synthèse, n°191, juin 2017, p3
[84] Chubb, est un consortium d'assurance et de réassurance issu du regroupement de 34 sociétés

Le monde maritime est un espace à haut risque où les assurances occupent une place très importante. L'assurance est née même du transport maritime avec le fameux « *prêt à la grosse aventure* ». L'assurance a toujours accompagné le transport maritime. Cependant, il est important de relever que l'arrivée des nouvelles technologiques avec la digitalisation des navires a renforcé les risques existants (défaillance informatique etc) et a créé de nouveaux risques (piratages, cyberattaques, espionnages etc).

Le risque cyber existe depuis longtemps mais les acteurs du monde maritime ont commencé à prendre conscience de son impact sur le secteur dans les années 2010. Pour le professeur O. LASMOLES[85], c'est au « *monde maritime de s'adapter aux risques et intégrer la cybersécurité de manière systématique dans ses réflexions mais surtout dans ses innovations.* » Cette adaptation devra permettre à l'industrie maritime d'avoir une vision qui s'oriente aussi vers la prévention et la protection des infrastructures contre le cyber-risque. En plus, la vulnérabilité des S.I dans les navires autonomes peut être deux (2) fois plus élevée du fait que dans le cadre des navires autonomes les intervenants se situent à terre. Ce qui peut permettre aux pirates de prendre possession du navire à distance sans que les opérateurs puissent intervenir.

La problématique du risque cyber dans les navires sans équipages devra être appréhendée de manière globale pour les assureurs car comme le souligne Nicolas Kamputais « *la technologie a permis au secteur maritime d'améliorer sa production, ses coûts ainsi que la réduction du temps d'acheminement. Néanmoins, les changements technologiques ont ouverts la porte à de nouvelles menaces et vulnérabilités, puisque le matériel est devenu accessible au monde extérieur*[86]. » Cette vulnérabilité flagrante montre que les navires sans équipages sont plus exposés aux risques cybernétiques.

Imaginons, un incident sur un navire autonome, la question de la preuve pourra être complexe. C'est à dire prouver s'il s'agit d'une cyberattaque ou d'une défaillance due à

[85] Lasmoles Olivier, Cybersécurité et navires sans équipages, DMF n°817, Octobre 2019, p777
[86] Nicolas Kampantais, Cyber Risks and Insurance in the marine Industry, http://www.jdsupra.com/legalnews/cyber-risks-and-insurance-in-the-marine-32124/, consulté le 7 juin 2020.

l'erreur de système ou de manipulation (système de télécommande par un humain à terre). Tous ces paramètres devront être pris en compte par les assureurs pour proposer un produit assurantiel qui satisfasse à une clientèle non convaincue de l'impact important des risques cyber sur leur économie.

Le risque pour les navires autonomes peut être plus complexe car ils s'appuient sur des capteurs (GPS, AIS, voire carte numérique) qui peuvent être plus facilement trompés[87].

La capacité d'analyse du risque en cas de sinistre, sa quantification pour la prime ou le calcul de sa probabilité sont autant d'éléments que les assureurs devront prendre en compte pour proposer un produit assurantiel efficace pour un risque aussi complexe et évolutif.

2) Vers une concrétisation de l'inassurabilité du risque cyber dans les navires autonomes?

Ici nous allons tenter de démontrer que s'il y a raison de parler de l'inassurabilité du risque cyber, c'est bien dans les navires autonomes que cela demeure pertinent. L'assurance des navires sans équipages peut être beaucoup plus complexe dans la mesure où il y a un principe fondamental dans les assurances qui est l'obligation pour l'assuré de prendre toutes les mesures nécessaires afin d'éviter l'aggravation du dommage. Comment, dans ce cas d'espèce, prendre des mesures pour éviter l'aggravation du dommage si l'on n'est pas à bord du navire? Comment des dispositions conservatoires des pertes et dommages peuvent être pris si le navire navigue seul sans humain pouvant intervenir sur place? Sommes-nous face à un scénario où le débat de l'inassurabilité du risque domine?

Pour répondre à ces questions, il serait judicieux pour les assureurs d'engager des études leur permettant de mieux cerner le risque ou de pouvoir intervenir avec des experts dans ce genre de situation. Mais tout cela peut affecter la prime d'assurance et rendra par la même occasion la couverture de ce risque trop chère pour les assurés. Reste à savoir si le risque cyber est assurable dans les navires autonomes.

Il est vrai que l'assurance se base sur des données historiques lui permettant de quantifier un risque et de fixer une prime. Mais dans le cas des navires autonomes, il

[87] https://www.marinelink.com/news/autonomous-shipping-cyber-hazards-ahead-471587

n'existe pas encore de données permettant aux assureurs de quantifier le risque. C'est la raison pour laquelle, et de manière générale, le risque cyberattaque est exclu des polices proposées, peu importe le type de navire. En effet, les assureurs ont sagement éclipsé ce risque de leur police en insérant automatiquement une clause d'exclusion des risques cyber.

Dans la police anglaise c'est la clause dite CL380:

« Institute cyber attack exclusion clause (CL380) 10/11/2003 :

1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system.

1.2 Where this Clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software programme, or any electronic system in the launch and/o guidance system and/or firing mechanism of any weapon or missile. »

Cette même clause a été traduit librement par la police française d'assurance maritime sur corps de tous navires - tous risques[88].

Traduction libre de la clause anglaise CL380

« *Clause additionnelle: Clause d'exclusion des risques cybernétiques*

1.1 Sous réserve des dispositions de l'article 2 ci-dessous, sont exclus les pertes et dommages, recours de tiers ou dépenses résultant directement ou indirectement de l'utilisation ou de l'exploitation, avec l'intention de causer des dommages, de tout ordinateur ou équipement informatique, programme ou logiciel informatique, programme malveillant, virus informatique ou processus informatique, ou tout autre système électronique.

[88] Fédération Française de l'assurance, Assurance Maritime sur corps de tous navires - tous risque/package modèles de polices et de clauses, Version française, 1 janvier 2012.

1.2 Si la présente clause fait l'objet d'un avenant à des garanties couvrant les risques de guerre, guerre civile, révolution, émeute, insurrection, ou conflit en résultant, ou tout acte d'hostilité effectué par ou contre une puissance belligérante, acte de terrorisme ou toute action menée par des personnes agissant pour un motif politique, l'article 1. ne pourra pas exclure les pertes - dans la mesure où elles sont couvertes - résultant de l'utilisation de tout ordinateur, équipement informatique ou programme ou logiciel informatique, ou de tout autre dispositif électronique installé dans le système de lancement et/ou de guidage, et/ou dans le mécanisme de mise à feu de tout arme ou missile. ».

On remarque que le risque cyber est exclu des polices anglaise et française, d'autant plus pour les navires autonomes ; car la couverture peut être envisagée dans les navires conventionnés par le biais des clauses additionnelles.

Le paradoxe est que le facteur risque humain est réduit, mais le risque de la cyberattaque est décuplé. Ainsi, la diminution de l'un permettra peut-être de compenser les coûts engendrés par l'incertitude des nouveaux risques.

Sous-section 2: La cyberdépendance des navires

La mutation de l'industrie maritime est accélérée par sa dépendance aux nouvelles technologies. Aujourd'hui, les opérations de transports maritimes sont inconcevables sans l'internet, les systèmes d'aide à la cargaison, embarqués ou satellitaires, et sans les différentes liaisons de communication reliant les navires aux ports[89]. La technologie devient de part et d'autre un élément indispensable dans le transport maritime du fait de la dépendance des navires aux nouvelles technologies (A). Mais des études récentes ont déjà démontré à travers des scénarios (B) que le risque cyber peut atteindre des dimensions incontrôlables à cause de la corrélation des risques (C)

A) La dépendance des navires aux nouvelles technologies

L'imagination des entreprises ne semble souffrir d'aucune limite pour simplifier, transformer et réinventer les usages de tous les acteurs de la vie économique en tirant parti

[89] Patrice A. EDORH-KOMANE, Les menaces cyber dans le secteur maritime: a-t-on déjà envisagé tous les scénarios? P.1

des très larges potentialités offertes par les outils numériques[90]. Cette tendance à vouloir aller plus vite dans les transactions et à gagner du temps dans les affaires nous rend « cyberdépendant » et n'est pas sans conséquences. Ces conséquences se justifient par le fait que derrière chaque facilité il y a un risque, et le risque de voir ses systèmes informatiques hackés devient de plus en plus important. Cela nous ramène à un scénario post-apocalyptique analogue à celui envisagé par Barjavel dans son roman *Ravage*[91]où l'électricité disparait. L'industrie maritime devra désormais faire face aux nouveaux risques sur lesquels s'adjoignent les risques traditionnels.

Cette dépendance des navires aux nouvelles technologies n'est pas sans risque car on assiste à une recrudescence des attaques cyber. Comme dans le terrestre et l'aérien, l'industrie maritime a enregistré plusieurs attaques cyber majeurs durant la dernière décennie. La particularité des attaques cyber dans le milieu maritime c'est qu'elles engendrent souvent des dommages à hauteur de milliard de dollars, ce qui n'est pas négligeable pour les assureurs et les acteurs maritimes. Ces attaques ont montré les menaces que le cyber-risque fait peser sur l'économie et la société.

Face à la multiplication des attaques cyber, les acteurs économiques disposent de deux outils, le recours à la prévention (cf. Infra) et le transfert du risque aux assureurs au cas où la prévention n'aurait pas suffi à se prémunir contre le cyber-risque.

Beaucoup de ces attaques ont montré que le risque cyber est de nature systémique[92], à cause de sa capacité à affecter un nombre important d'entreprises simultanément. Il est évident que les événements cyber peuvent entrainer des conséquences beaucoup plus graves que celles qu'on a connues jusqu'à présent.

[90] Gaspard FEREY, Nicolas GROROD, Somin LEGUIL, L'assurance des risques cyber, comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive?
[91] R. Barjavel, Ravage, 1943.
[92] Cyber Risk Management, Report 2019

B) Du concret: le scénario du Shen Attack

Dans une étude réalisée par l'université technologique de Nanyang au Singapur, en collaboration avec le Cambridge Center for Risk Studies, via le projet Cyber Risk Management *(CyRiM),* les experts ont démontré deux scénarios d'attaques cyber que sont le *Shen Attack* et le *Bashe Attack,* pour mettre en évidence les conséquences d'une cyber attaque systémique de grande ampleur sur l'économie globale et le marché de l'assurance.

Dans ce mémoire, nous allons étudier seulement le scénario du *Shen Attack,* qui est spécifique au secteur maritime, contrairement au *Bashe Attack,* qui sans précision de secteur, offre une vision générale de ce qui pourrait être les conséquences d'une infection généralisée à travers un maliciel contagieux. Notons que ce dernier a démontré à l'échelle mondiale, des pertes et dommages, allant de 85 à 193 milliards de dollars, dont 10 à 27 milliards de dollars pour le marché de l'assurance[93].

Intéressons-nous plus au scénario de *Shen Attack*[94], qui concerne directement le secteur maritime. Il relève trois hypothèses d'attaque cyber sur les systèmes d'information d'une société de gestion de flottes de navires ayant des connexions avec les plus grands ports de la région Asie-pacifique, fréquentés par les navires qu'elle a à charge. Rappelons que les sociétés de gestion de flottes offrent une large variété de service au profit des armateurs, comprenant ainsi la mise à disposition d'équipage, des inspections techniques, l'organisation des voyages etc. Elles peuvent également avoir à gérer des flottes de plusieurs centaines de navires. On peut donner l'exemple du géant mondial du *Shipmanagement, V.Group*, qui assure une flotte de 940 navires à travers 30 pays dans le monde[95].

L'objectif du *Shen Attack* est de mettre en évidence les impacts d'une attaque cyber systémique sur l'économie mondiale et le niveau du marché de l'assurance cyber dans le secteur maritime.

[93] Patrice A. EDORH-KOMANE, Les menaces cyber dans le secteur maritime: a-t-on déjà envisagé tous les scénarios? P.2
[94] Cyber Risk Management, report 2019
[95] Lloyd's 2018

Il est maintenant important pour nous de démontrer comment le scénario du *Shen Attack* est mis en place. D'abord c'est un virus qui infecte les systèmes informatiques de la société de gestion de flottes de navires; ensuite il se propage et affecte tous les navires de la flotte en activité; enfin le virus s'étend, grâce aux liaisons de communication, à tous les ports fréquentés par les navires infectés[96]. La propagation du virus se fait de manière exponentielle grâce au contact numérique entre les navires. Cette propagation est rendue possible dans la mesure où désormais, beaucoup d'échanges de données entre navires et ports fréquentés s'effectuent par voie électronique.

Ce scénario du *Shen Attack* montre la cyberdépendance des navires et par conséquent rend de plus en plus vulnérable les systèmes d'information des navires. Un teste a été effectué sur des ports se trouvant dans la région d'Asie-Pacifique. Dans la première hypothèse, l'attaque a affecté des ports Japonais, Malaisiens, et Singapouriens. Dans la deuxième hypothèse, des ports Coréens sont ajoutés à la première liste et enfin la troisième hypothèse, la plus extrême, l'attaque a affecté des ports chinois[97]. Au total 15 ports ont été touchés par l'attaque et ont tous dû être fermés. Les pertes économiques subies directement ou indirectement sont estimées à plus de 200 milliards de dollars. Cela concerne les dommages aux marchandises périssables (pertes directes) mais également la suspension de la production et des exportations, du fait de l'attaque.

Pour les assureurs, trois types de couvertures sont en cause: le premier c'est les polices cyber ordinaires qui couvrent les pertes de données, les responsabilités, les dommages aux biens et d'autres partes résultant de la défaillance des systèmes de communication, accidentelle ou non. Le deuxième concerne les polices ordinaires qui contiennent des clauses d'exclusion des risques cyber qui pourraient cependant être affectées du fait que la clause n'est pas par exemple précise ou complète pour exclure totalement toutes les conséquences potentielles d'une attaque cyber. Le troisième type de couverture regroupe les polices d'assurance « tous risques » qui, le cas échéant, ne comportent aucune exclusion des risques cyber.

[96] CyRiM Shen Attack Final Report 2019
[97] Shen Attack: Cyber Risk in Asia Pacific ports

Dans le cas d'une attaque cyber, en plus de la première catégorie qui devra naturellement être mise en œuvre, les deux dernières vont l'être aussi pour ce qui est convenu d'appeler « *couverture silencieuse* ». En cas de sinistre cyber, il arrive que certaines conséquences soient couvertes par des polices d'assurance dommages ou responsabilité civile classique, qui incluent ou excluent, parfois de manière implicite ou ambiguë, les risques cyber, par le biais des « *couvertures silencieuse* ». Nous n'allons pas plus loin sur cette question des couvertures silencieuse qui fera l'objet d'étude dans la deuxième partie de ce mémoire.

En conclusion, on peut dire que le scénario du *Shen Attack* montre que la quasi-totalité des secteurs d'activités sont exposés, au moins par ricochet, aux effets des attaques cyber. Cela s'explique par le fait que la majeure partie des entreprises utilisent les mêmes outils de stockages ou de communication, et de ce fait, entraine une corrélation des risques.

C) La corrélation des risques

En assurance il existe un principe fondamental, qui permet à l'assureur de prévoir la perte moyenne par assuré en appliquant la loi du plus grand nombre selon laquelle l'indemnité moyenne par assuré, si elle est aléatoire, n'en est pas moins constante, lorsque les dommages sont distribués de manière identique et indépendante [98] . C'est la mutualisation des risques. Or, dans le cyber-risque, la réalité est tout autre car la cyberdépendance des systèmes informatiques, étant un élément qui accélère la propagation du virus, peut faire obstacle à l'application de la loi du grand nombre. Par exemple un virus informatique est capable de s'auto-répliquer dans un programme légitime et passer d'un ordinateur à un autre en infectant les systèmes qu'il rencontre.

En outre, contrairement au virus biologique, qui se transmet d'un individu à un autre, le virus informatique se transmet à partir d'un seul nœud à *n* d'ordinateurs de plusieurs entreprises[99]. Cette capacité à se propager dans des milliers d'ordinateurs peut s'illustrer dans l'affaire *Notpetya,* où l'auteur s'est servi de la procédure de mise à jour d'un logiciel de comptabilité en Ukraine pour infecter plusieurs cibles, dont l'aéroport de Kiev, le système de surveillance des radiations de la centrale nucléaire de Tchernobyl, la

[98] Club des juristes, Assurer le risque Cyber, Janvier 2018
[99] A. JAGHADAM, « Les conditions d'assurabilité des cyber-risques », Revue *Risque*, no 77, 2009.

Russie, le Royaume-Uni, la Norvège, les Pays-Bas ou la France. Et tout cela en moins de cinq heures après la première détection du virus. On note une corrélation des risques qui est causée par la vulnérabilité des systèmes et leur cyberdépendance. On peut donc remarquer que l'impact que peut causer un cyber attaque est juste impressionnant sur le plan économique et industriel. Mais qu'en est-il des assureurs? Quel est leur rôle dans la prise en charge des risques cyber? S'agit-il d'un risque nouveau dont les paramètres de corrélation sont méconnus de tous les acteurs? Une chose est sûre, la corrélation des risques, pose un double défi aux assureurs[100].

D'une part, la garantie de leur solvabilité peut faire défaut en raison de la complexité de leur stratégie de diversification du portefeuille de risques. Notons que la diversification géographique des risques dans le cadre de la mutualisation est presque impossible puisque les incidents cyber peuvent être transfrontières. Contrairement aux risques de catastrophes naturelles, dont l'impact est généralement confiné dans un espace régional, les conséquences du risque cyber peuvent atteindre des proportions plus importantes. Par exemple la cyberattaque lancée contre l'Estonie[101], en 2007, est une illustration parfaite de l'étendue d'une cyberattaque sur le plan national. Sur le plan international nous avons les deux plus grandes cyberattaques où « le monde entier devient une zone de cumul[102] ».

D'autre part, la corrélation entre un grand nombre de risques rend la quantification du risque et la définition de la prime d'assurance beaucoup plus complexes[103]. En effet, la proportion de contamination est trop importante car, il suffit qu'un maillon de la chaine soit affecté pour condamner tout le système. Cela voudrait dire que malgré les efforts de protection et de prévention que peut mettre en place les acteurs, la faille peut provenir de n'importe quel serveur ayant eu contact avec le navire ou les infrastructures à terre (sous-traitant, clients, ports).

Dans une conférence animé par H. KUNREUTHER, E. MICHEL-KERJAN, en 2004 sur l'assurabilité du risque terroriste (I*nsurability of (mega-) Terrorism risk:*

[100] Club des juristes, Assurer le risque Cyber, Janvier 2018, p26
[101] https://www.lemonde.fr/europe/article/2007/06/27/l-estonie-tire-les-lecons-des-cyberattaques-massives-lancees-contre-elle-pendant-la-crise-avec-la-russie_928568_3214.html
[102] A. JAGHADAM, « Les conditions d'assurabilité des cyber-risques », Revue Risque, no 77, 2009, note 5
[103] Club des juristes, Assurer le risque Cyber, Janvier 2018, p26

Challenges and Perspectives [104] *),* la notion de « *sécurité interdépendante* » pour caractériser le risque terroriste, pourrait aussi être pertinent dans le cadre du cyber-risque. Ainsi, une sécurité portuaire inadéquate peut faciliter une attaque cyber de navire, quel que soit les mesures de sécurité prises par le navire.

Dans le rapport[105] publié en janvier 2018, le Club des juristes explique que « *ces interdépendances entre systèmes informatiques augmentent de façon exponentielles dans nos sociétés de plus en plus numériques: l'extension du périmètre de la transformation numérique des organisations, la corrélation entre des millions d'utilisateurs hyper connectés dans l'architecture d'internet, l'utilisation généralisée de logiciels susceptibles de se révéler vulnérables, l'exposition du nombre de dispositions connectés et le recours au Cloud sont autant de catalyseurs majeurs de la corrélation des risques* ». On remarque donc que la digitalisation des navires a fortement accéléré le risque cyber dans les compagnies maritimes. Cette corrélation des risques demeure donc une source d'incertitude et de cumul et rend indéniablement plus complexe la définition d'une offre d'assurance cyber pertinente.

Les cyber risques sont souvent très interdépendants: un système affecté peut augmenter la vulnérabilité d'autres systèmes au sein d'une même entreprise. Ainsi une attaque réussie contre une entreprise peut affecter d'autres. La migration des services informatiques des entreprises vers le Cloud augmente le risque de problèmes corrélés entre eux en cas d'attaque cyber sur les principaux produits. Toutefois, le degré de dépendance varie selon le type de cyber-menace [106]. Par contre, lorsque l'attaque implique des interactions des utilisateurs, telles que le phishing (hameçonnage) pour les logiciels malveillants, ceci peut entrainer des vulnérabilités corrélées entre les entreprises.

Il est donc important pour les assureurs de maitriser toutes ces données afin d'apporter des solutions assurantielles et de lancer des conversations précises et claires avec les clients.

[104] H. KUNREUTHER, E. MICHEL-KERJAN, Insurability of (mega) terrorism risk : challenges and perspectives in OECD (2004).
[105] Club des juristes, Assurer le risque cyber, janvier 2018, p28.
[106] Swiss Re, Cyber : getting to grips with a complex risk, in Sigma 1/2017 p. 19.

Le cyber-risque est un marché où les assureurs ont des opportunités à exploiter mais son développement nécessite une collaboration des assureurs et des assurés afin de pallier à la vulnérabilité des navires. C'est ce qu'illustrait Angela Kelly[107] dans un article de presse publié dans le Lloyd's, en date du 29 octobre 2019. En effet, selon elle «*Le cyber-risque est l'un des défis les plus critiques et complexes auxquels l'industrie maritime de l'Asie-Pacifique est confrontée aujourd'hui. Comme ce risque augmente avec l'application croissante de la technologie et de l'automatisation dans l'industrie, la collaboration et la planification future par les assureurs et les gestionnaires des risques sont essentielles.* » Ceci étant, le marché de la cyberassurance ne peut se développer que si les acteurs acceptent d'entretenir une collaboration afin de rattraper leur retard sur le marché du cyber-risque.

Le rôle des assureurs est primordial sur ce marché, encore méconnu. Il doit apporter une solution assurantielle permettant de couvrir les processus critiques des entreprises dans le transport maritime et de garantir leur résilience en absorbant les conséquences financières d'un éventuel sinistre cyber. Toutefois, il faut relever que la transformation numérique accélérée du monde maritime a complexifié la quantification du risque cyber. Cette digitalisation a entrainé une dépendance forte des navires à leur système informatique dont la disponibilité, la confidentialité, et l'intégrité sont devenues nécessaires à leur exploitation[108].

[107]Angela Kelly, Singapore Country Manager, Lloyd's, Single cyber attack on Asia-Pac ports could cost $110bn, equal to half of all 2018 natural disasters.

[108] Gaspard FEREY, Nicolas GROROD, Somin LEGUIL, L'assurance des risques cyber, comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive?

CONCLUSION :

Le risque cyber est une préoccupation majeure des compagnies maritimes. Ces 3 dernières années ont été le déclic d’une prise de conscience importante des acteurs du secteur maritime. L’intervention des assureurs était alors primordiale. Mais face à un nouveau risque dont la base de données est manquante, son assurabilité peut être problématique. D’une part les assureurs se basent sur des statistique pour évaluer la probabilité d’occurrence d’un risque et son impact potentiel, d’autre part le réglementation est en phase d’adaptation aux enjeux du marché.

Cependant on note de nombreux points positifs dans le futur de l’assurabilité du risque cyber. D’abord les Etats et Organismes internationales accompagnement activement les compagnies maritimes dans le renforcement du niveau de sécurité. La réglementation peut être un catalyseur du changement. À l’image de BIMCO qui a établie plusieurs recommandations pour orienter les compagnies dans la gestion des cyber-risques. Ensuite, les assureurs une fois rassurés de la maturité du niveau de sécurité des compagnies maritime, pourront enfin évaluer leur cyber-exposition et proposer une solution assurantielle adaptée aux besoins des clients.

Reconnaissant le potentiel du marché les assureurs se préparent pour faire face aux enjeux du marché. Au regard de l’avancée de la technologie, il est fort probable que le risque cyber soit dans un futur proche une pierre angulaire de l’offre d’assurance. C’est la raison pour laquelle de nombreux assureurs et réassureurs commencent à investir sur le marché de l’assurance cyber.

PARTIE II. L'ENGAGEMENT DES ASSUREURS POUR LA PRISE EN CHARGE DU RISQUE CYBER

Il est maintenant clair qu'assureurs et réassureurs reconnaissent la complexité du risque cyber. Mais au regard des opportunités que peut offrir le marché de l'assurance cyber, beaucoup d'assureurs s'engagent à couvrir ce risque malgré les obstacles que peut engendrer sa prise en charge. Pour cela, il faudra tout de même relever certains défis pouvant faciliter la gestion du risque (**Chapitre 1er**). L'enjeu est de taille; mais le monde maritime a besoin de l'accompagnement des assureurs et réassureurs pour faire face à ce risque. Cet accompagnement se fait par la mise en place de stratégies et de solutions adaptées aux besoins des compagnies maritimes (**Chapitre 2**).

CHAPITRE 1er. LES NOUVEAUX DÉFIS DANS LA GESTION DU RISQUE CYBER

La gestion des cyber-risques est une activité complexe, avec des composantes technique, humaine et organisationnelle. Pour se faire les assureurs doivent planifiés une approche technique globale pour mieux analyser le risque dans toutes ses dimensions (**Section 1).** Mais en plus de cette approche technique, les acteurs économiques doivent se montrer plus engagés sur ce terrain en augmentant la capacité du marché **(Section 2**).

SECTION 1: CENTRER L'APPROCHE TECHNIQUE POUR L'ANALYSE DU RISQUE

La cybermenace n'épargne plus aucune entreprise ni aucun secteur d'activité. Afin d'y faire face, les entreprises doivent, en amont, renforcer leur niveau de sécurité, pour ensuite le transférer vers le marché de l'assurance. Dans le secteur maritime, les assureurs sont très réticents pour ce risque en raison du problème de cumuls des risques et de la couverture silencieuse (**Sous-section 1**). C'est la raison pour laquelle la plupart des assureurs et réassureurs s'investissent surtout dans le renforcement des mesures de prévention (**Sous-section 2**).

Sous-section1: Le cumul des risques et la couverture silencieuse : Un casse-tête pour les assureurs

Les risques technologiques liés à la numérisation des navires deviennent de plus en plus fréquents mais les assureurs conscients des potentiels de ce marché, tentent de trouver une solution assurantielle sur mesure pour ces risques. Tout de même, il faut au préalable résoudre la problématique de cumuls (A) et des couvertures silencieuses(B).

A: La maitrise de cumuls des risques

1) L'encadrement de la technique informatique

Après avoir démontré la complexité du risque cyber dans tous ses aspects, il serait pertinent de démontrer que malgré son caractère complexe, les assureurs « *peuvent venir à bout du cyber-risque* [109] ». Il existe un principe essentiel en assurance qui est la mutualisation. Elle consiste à regrouper un nombre suffisamment important de risques indépendants afin de réduire l'éventualité d'une indemnisation simultanée de plusieurs assurés pour un même risque. Dans le cadre du risque cyber, c'est un énorme défi que les assureurs doivent relever, car le risque cyber est un risque potentiellement systémique qui peut toucher un grand nombre de clients ou même déclencher de multiples sinistres chez un client. Par exemple une seule attaque cyber peut engendrer un risque réputationnel, un dommage aux biens, une responsabilité civile professionnelle ou encore une responsabilité civile de mandataires sociaux. Cette multitude de conséquences doit être mesurée par les assureurs pour réduire leur exposition au titre d'un même incident.

De plus, l'interconnexion des systèmes informatiques a comme conséquence le fait que les cyber-incidents soient en mesure de toucher plusieurs produits d'assurance et polices indépendantes selon un mécanisme de chaîne similaire à la couverture CBI[110] (Contingent Business Interruption).

Dans l'assurance maritime, la charge de sinistre globale pour le risque cyber peut avoir diverses sources n'ayant aucun lien entre eux et pouvant affecter plusieurs assurés. On remarque que la plupart des assurés se tournent vers le même prestataire informatique.

[109]Swissre, Cyber: Comment venir à bout d'un risque complexe?, Sigma n°1, 2017.
[110] Cyber resilience: The cyber risk challenge and the role of assurance, CRO Forum, Décembre 2014.

Ce qui en soi, augmente le risque de corrélation en cas d'attaque cyber touchant des points clés du réseau. En effet, la cause de corrélation des sinistres est parfois difficile à identifier. Ce qui ne facilite pas le traitement des sinistres par les assureurs. Les assureurs peuvent perdre beaucoup de temps dans l'identification de la cause de corrélation sans même être sûrs de comprendre le cheminement exact. Dans ces conditions, les assureurs ont du mal à différencier, dans la masse de demandes, entre les sinistres qui sont à rattacher à la même cause fondamentale et ceux qui ont une autre origine.[111]

La question du cumul est un réel problème qui dissuade les assureurs et réassureurs dans la prise en charge du risque cyber. En effet, selon la récente étude de Swiss re: « *le potentiel de cumul dommageable est une contrainte essentielle pour l'appétit au risque des assureurs qui s'intéressent aux cyber-risques, et l'est d'autant plus pour les réassureurs, qui se tiennent prêts à absorber les pertes extrêmes de plusieurs cédantes*[112]. » La maitrise du cumul semble alors primordiale dans la mesure où cela éviterait aux assureurs et réassureurs d'avoir des pertes catastrophiques qui pourraient épuiser leur capital ou même faire face à un risque d'insolvabilité. Elle est également cruciale pour l'assureur qui doit comprendre l'environnement contractuel au regard de l'état de l'art de la technique informatique et au regard du droit informationnel ou du numérique qui évolue[113]. Cela lui permettrait d'avoir une meilleure gestion de l'accumulation des risques.

2) La gestion de l'accumulation de risques

En janvier 2017, le groupe RMS, leader mondial de la gestion des risques de catastrophe, a mis en place un outil permettant aux assureurs de modéliser une gamme de cyber-catastrophe potentielle afin de déterminer l'impact potentiel d'une attaque systémique à grande échelle. Ce système permet également aux assureurs d'identifier et de gérer les accumulations potentielles de risque cyber dans leurs portefeuilles. Selon Christer Pehrson, directeur général du développement client chez RMS: « les accumulations *de risques cyber sont extrêmement complexes et non limitées géographiquement,*

[111]Swissre, Cyber: Comment venir à bout d'un risque complexe?, Sigma n°1, 2017, p20.
[112]*Ibid, p21*
[113]« La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance », System X, Institut de recherche Technologique, Rapport, 2016, p39.

contrairement aux périls tels que les ouragans ou les tremblements de terre. » Ce qui veut dire que la chaîne de l'impact et des pertes potentiel peut être insupportable. Cette accumulation croissante de risques au sein de leur activité de cyberassurance préoccupe de plus en plus les assureurs.

Dans leur rapport sur l'assurance du risque cyber, le Club des Juristes, détaille les problèmes auxquels font face les réassureurs. Il démontre qu'il y a un risque de corrélation d'un même incident cyber sur plusieurs contrats de réassurance et qu'un incident cyber chez un assuré peut être indemnisé au titre de plusieurs contrats d'assurance[114]. C'est pourquoi les assureurs et réassureurs ont besoin de connaitre la capacité de gestion du risque cyber par les entreprises. Cela leur permet de pouvoir évaluer leur exposition et d'établir une cartographie du risque potentiel d'accumulation.

Parallèlement certains assureurs et réassureur optent pour la mise en place de scénarios de cyber-catastrophiques. De manière plus concrète, ces scénarios se basent sur des incidents de grande ampleur avec des estimations d'impact financier globales. Mais les scénarios doivent demeurer probables, c'est à dire ne pas s'aventurer sur des scénarios « fin du monde » et permettre d'estimer l'impact sur l'économie et sur les réassureurs[115]. Mais, à l'heure actuelle, il est difficile pour les assureurs maritimes de fixer leurs niveaux de capacité du fait qu'il n'y ait pas encore d'événement cyber qui cible particulièrement le secteur. Il est à noter qu'au regard de l'évolution de la technologie et de la cyberdépendance des compagnies maritimes, le secteur maritime est, comme tous les autres secteurs, très exposé aux risques cyber, s'il n'est pas des plus exposés.

Pour l'instant, il est mieux pour les assureurs d'adopter une vision prudente du risque, car ils sont incapables, actuellement, de définir la perte maximale probable d'un incident cyber. Cela peut certes freiner le développement du marché en raison du manque d'information dans ce domaine, mais semble moins risqué sur un terrain mal connu.

[114] « Assurer le risque cyber », Club des Juristes, Rapport, Janvier 2018, p87.
[115] *Ibid*, p88.

B) La problématique des couvertures silencieuses

1) L'identification des polices traditionnelles « silencieusement » exposé au risque cyber

Le marché de l'assurance cyber est un marché très prometteur compte tenu de la nature évolutive du risque, de l'omniprésence du numérique, de la réglementation en expansion et de la valeur de l'assureur en tant qu'outil de gestion des risques. Pourtant, le marché peine à développer en raison de plusieurs facteurs qui freinent son décollage. Au-delà des problématiques de cumuls, il existe d'autres facteurs plus complexes comme la couverture « silencieuse ».

La couverture « silencieuse » est, en effet, l'une des principales difficultés auxquelles les compagnies d'assurance doivent faire face. Ainsi, en cas d'incident cyber, il peut arriver que certaines conséquences soient couvertes par des polices d'assurance dommage ou RC classique, qui incluent ou excluent, de manière parfois implicite ou ambiguë, les risques cyber. Ce qui veut dire que la plupart des polices traditionnelles sont « silencieusement » exposées aux risques cyber. Or, l'objectif est de trouver une solution assurantielle plus adaptée, permettant ainsi aux assureurs d'évaluer leur cyber-exposition. C'est ce qu'indique l'agence de notation Moody's Investors Services sur la cyberassurance qui estime qu'« *une évaluation et une gestion précise de la cyber-exposition constitue une priorité absolue pour les assureurs dommages, d'autant que les limites de garantie des polices traditionnelles sont souvent des multiples de celles prévues par les polices cyber dédiées* ». Cette priorité est d'autant plus urgente dans la mesure où les conséquences cyber sont financièrement élevées et il serait très difficile pour les assureurs et réassureurs de gérer un sinistre cyber de grande ampleur « silencieusement » couvert par une police traditionnelle.

Les compagnies d'assurance doivent se pencher sérieusement sur la question avant de faire face à des situations où une attaque cyber serait couverte par défaut d'exclusion. D'autant plus que certains assurés, partant du principe simplificateur que l'ambiguïté leur sera favorable, s'estiment correctement protégés et refusent de se pencher sur cette

problématique ou de mettre à jour leur couverture afin de prendre correctement en compte l'impact du cyber sur leur besoin assurantiel[116].

Il serait alors plus prudent pour les assureurs et réassureurs de mesurer leur cyber-exposition dans les contrats déjà souscrits et de clarifier les contrats futurs dans le but d'exclure toute éventuelle couverture de sinistre, qu'il soit cyber ou non.

2) La clarification des contrats d'assurance

Beaucoup de compagnies commencent à s'organiser en prenant des mesures contre les couvertures silencieuses, à l'image d'Allianz (via AGCS), ou du régulateur Britannique (The Bank of England Prudential Régulation Authority) qui a demandé aux assureurs d'élaborer des plans d'action en ce sens. Cette organisation a jugé implicite l'exposition « silencieuse » des assureurs au cyber-risque dans les polices « tous risques » et autres polices RC[117].

En plus, la « *silent cover* » fait peser sur les assureurs d'énormes risques et c'est d'ailleurs ce qui a poussé le Lloyd's de Londres à se pencher sur la question de la menace « silencieuse ». A ce titre, il appelle ses membres à clarifier leurs contrats d'assurance et de réassurance pour éviter les cyber-expositions cachées. Ils doivent dorénavant dire explicitement ; s'ils prévoient la couverture des cyber-risques, et le cas échéant, jusqu'à quel niveau. Cela permettrait au moins d'éviter l'ambiguïté au moment de la souscription, car « *la logique qui prévaut pour l'instant est que les cyber-risques sont souvent couverts par le simple fait de ne pas être exclus*[118] » souligne John Neal, directeur général du Lloyd's; avant de rajouter qu' « *il n'y a aucun problème à couvrir ce type de risque. Mais nous devons être totalement transparents vis-à-vis du client, qui doit savoir son niveau de protection. Et nous devons connaître notre exposition, afin de pouvoir ensuite la gérer* ».

Par ailleurs dans l'affaire qui opposait Mondelez, le géant américain du chocolat et du biscuit et l'assureur Zurich, à la suite de l'attaque cyber mondial *Notpetya* de juin 2017,

[116] Gaspard Ferey, Nicolas Grorod, Simon Leguil, « L'assurance des risques cyber, Comment tirer la meilleure partie de l'assurance dans un contexte de numérisation intensive? », Mémoire de fin de formation du corps des mines, Paris Tech, 2017, p45.
[117] Swiss re, Cyber: Comment venir à bout d'un risque complexe?, Sigma n°1, 2017, p16.
[118] https://www.lesechos.fr/monde/europe/cyber-risques-le-lloyds-de-londres-veut-mettre-de-lordre-dans-les-contrats-1132705

l'assuré estimait que son contrat d'assurance dommages couvrait « *les dommages et sinistres physiques causés aux données électroniques, aux programmes et aux logiciels, incluant [ceux] résultant de l'introduction malintentionnée de codes machine ou d'instruction* [119]». Toutefois, l'assureur évoquait l'exclusion « *pour les actes hostiles ou liés à des guerres « warlike » ou causés par « un gouvernement ou une force souveraine* ». On remarque que l'assureur évoque une clause de guerre pour un sinistre lié à la cyberattaque. L'affaire est toujours en cours devant la justice américaine, mais ce qui est sûr c'est que son dénouement aura un enjeu capital tant du côté des assurés « dans la certitude des couvertures[120] » que de celui des assureurs dans la nécessité de cartographier la « cyberexposition », c'est-à-dire l'ensemble des prises en charge prévues dans leurs portefeuilles en matière de couverture du risque cyber[121].

Les assureurs doivent maintenant prendre en considération tous les scénarios probables d'attaques cyber. Ce qui nécessite une ressource humaine spécialisée afin de passer en revue tous leurs contrats existants pour savoir si oui ou non les risques cyber sont incluent. L′objectif pour les assureurs est d′arriver à un niveau de maîtrise du risque, leur permettant d′exclure toutes les clauses pouvant entrainer la couverture d′un événement cyber par les polices traditionnelles, et de proposer des garanties spéciales complémentaires. A l′heure actuelle, très peu d′entreprises sont spécialisées au cyber. Tout de même, dans un futur proche, il est indéniable que le risque cyber fera partie des piliers majeurs de l′assurance. L'on se demande alors si les assureurs ne devraient-ils pas envisager la création d′une police « cyber » au même titre que les polices dommages ou RC ? Mais, il faut au préalable, gagner la conquête de la maîtrise technologique, leur permettant de mieux appréhender le risque.

Toutefois, le marché cyber ne peut se développer que si les assureurs sont épaulés par des organisations, leur permettant d'anticiper les choses.

[119]Thévenin L., « Cybersécurité : le dossier qui agite assureurs et industriels », Les Échos, 11 janv. 2019.
[120]*Ibid.*
[121] Michel Séjean, « La cyberassurance, un contrat encore méconnu des entreprises », Gazette du palais, 5 mai 2020, n°376c5, P10.

Sous-section 2: Le renforcement des mesures de prévention

La meilleure manière de se prémunir contre un risque c'est d'anticiper des stratégies pouvant éviter sa survenance. De ce fait, les assureurs et réassureurs doivent collaborer avec d'autres acteurs certifiés (A). Cette collaboration peut permettre aux assureurs de mieux connaître le niveau de gestion du risque par les compagnies maritimes et d'évaluer leur exposition au risque cyber (B).

A: La collaboration d'autres acteurs certifiés

1) L'appui des sociétés de classification dans la prévention

La question de la sécurisation des navires face aux risques cyber doit aussi se passer de prime à bord chez les sociétés de classification. Elles jouent un rôle important dans ce bouleversement technologique et culturel. L'OMI et l'Association Internationale des sociétés de classification (IACS) ont une mission de régulateur qui doit impérativement fixer de hauts niveaux d'exigences pour les navires en matière de cybersécurité ; notamment dans le partage, la fusion des données issues de systèmes différents, la confiance dans les capteurs, l'intelligence artificielle et le cloisonnement et la redondance des réseaux et capteurs. Ainsi, au regard de ce qui précède, les sociétés de classification ont un rôle moteur à jouer dans la prévention des risques cyber.

Plusieurs recommandations ont été publiées par l'OMI et l'IACS dans le cadre de la gestion des risques liés à la cybersécurité. Au niveau de l'IACS, il y a une norme obligatoire appelée « On Board Use and Application of Computer based systems[122] ». Cette norme s'applique à la conception, à la construction, à la mise en service et à la maintenance des systèmes informatiques lorsqu'ils dépendent de logiciels pour la bonne exécution de leurs fonctions. Cela permet au navire d'avoir un système informatique qui fournit des fonctions de contrôle, d'alarme, de surveillance, de sécurité ou de communication interne qui sont soumises à des exigences de classification.

Toutefois, il est important de noter que la norme UR-E22 ne traite que des questions liées à la défaillance des systèmes informatiques mais ne concerne pas les

[122] UR E22, On board use and application of computer basedsystems- Rev.2 June 2016.

attaques volontaires. Certes la norme ne vise pas directement les attaques cyber volontaires, mais nous savons que le risque cyber n'est pas que malveillant. On peut même se placer dans un scénario où les hackers, profitent d'un bug informatique ou d'une erreur humaine, pour s'introduire dans les systèmes informatiques du navire ou voler des données.

En outre, le Bureau Veritas a développé plusieurs normes concernant la migration vers de nouveaux logiciels, la prévention des cyber attaques liés aux échanges de données entre la mer et la terre. Il accompagne les acteurs de l'industrie maritime à mieux se protéger contre les risques cyber. A titre illustratif, le leader du support maritime aux installations pétrolières, Bourbon, a accéléré la digitalisation de sa flotte avec l'appui du Bureau Veritas. Ils ont développé et déployé l'automatisation de certaines tâches, le contrôle à distance en temps réel ainsi que des technologies innovantes de navigation, tout en travaillant sur les sujets de cybersécurité.

Cette tendance de collaboration entre les acteurs du secteur maritime doit s'étendre aussi aux assureurs, car le transfert du risque cyber vers les assurances devient de plus en plus recommandé et la prise en charge d'un tel risque par les assureurs nécessite une collaboration avec les sociétés de classification qui œuvrent pour la sécurisation technologique des navires.

2) L'appui de l'ANSSI dans le renforcement de la relation de confiance entre assurés et assureurs

Le risque cyber est un risque dont la prise en charge nécessite la communication par le client de certaines informations parfois très confidentielles. D'une part, les assureurs ont besoin de connaître le système d'information des assurés afin de mesurer leur vulnérabilité et d'autre part, les assurés tiennent beaucoup à la confidentialité de leurs informations. L'intervention d'un tiers sera donc indispensable pour renforcer la relation de confiance entre assureurs et assurés dans la gestion des contrats cyber.

Les assurés ont besoin d'un climat de confiance et de confidentialité leur permettant d'informer les assureurs en toute transparence et de manière exhaustive pour réaliser le transfert de leur risque de manière optimale et être indemnisés dans les meilleurs

conditions[123]. Ce climat de confiance ne peut être établi que par une organisation intermédiaire pour maintenir l'équilibre entre les parties. En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est pertinente pour jouer ce rôle d'intermédiaire. En effet, l'ANSSI peut établir une charte type, engageant l'assureur à respecter la confidentialité et la sécurité des informations partagées par l'assuré à la souscription du contrat et lors de la gestion d'un sinistre[124]. C'est dans cette logique que s'inscrit l'ANSSI pour fournir le cadre confidentiel nécessaire aux échanges entre assureurs et assurés.

La coopération des assureurs avec l'ANSSI permettra ainsi de mettre en place une plate-forme sur laquelle toutes les informations en relation aux incidents cyber seront enregistrées.

De plus, les assureurs peuvent exploiter des données collectées par les pouvoirs publics par les biais d'agences et de réseaux supranationaux. En effet, l'action des pouvoirs publics ne se limite pas au partage des informations. Ils ont aussi un rôle à jouer dans l'élaboration de normes détaillées pour la promotion de systèmes informatiques hautement sécurisés. Ces normes peuvent être, pour les assureurs, un outil dont ils peuvent se saisir pour évaluer la solidité des contrôles internes des compagnies maritimes et pour mieux appréhender leur résilience face aux cyber risques. Par exemple, le National Institute of Standards and Technology (NIST) aux Etats-Unis et la norme ISO 27001[125] sont des outils mis à la disposition des entreprises, leur permettant « *d'évaluer et d'améliorer leur propre cyber-sécurité*[126]. » En plus, cela permettrait aux assureurs de préparer leur cyber-exposition et de proposer un produit assurantiel conforme aux besoins des clients.

[123] Philippe Cotelle, Philippe Wolf, BénédicteSuzan. « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance ». [Rapport de recherche] 401, IRT SystemX. 2016.
[124] « Assurer le risque cyber », club des Juristes, Rapport, Janvier 2018, p93.
[125] ISO/IEC 27001, Technologies de l'information, Techniques de sécurité, Systèmes de management de la sécurité de l'information, Exigences, 2013.
[126]Swissre, Cyber: Comment venir à bout d'un risque complexe? Sigma n°1, 2017, p36.

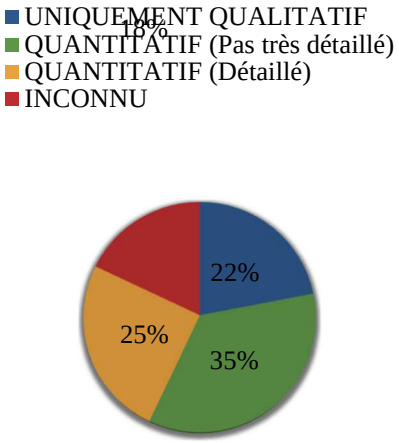
B: La capacité d'évaluer l'exposition au risque cyber

1) Le stress test

La prévention ne peut être efficace que si les compagnies maritimes et les assureurs disposent d'outils leur permettant d'évaluer leur taux d'exposition aux risques cyber. En effet compte tenu de la complexité de quantification du risque cyber, les assureurs doivent adopter une approche plus profonde de la modélisation. Avec la digitalisation, les attaques deviennent plus intenses, tant par leur fréquence, que par les coûts qu'elles engendrent. Dans une récente étude dirigé par *SANS Institute*, une organisation de professionnels de la sécurité, on se rend compte que seul 25% des entreprises utilisent des modèles quantitatifs détaillés pour les cyber risques, alors que la majorité d'entre elles utilisent des modèles simples ou uniquement qualitatifs. Cela veut dire que la majeure partie des entreprises minimisent encore le risque cyber. Egalement, il ressort d'une autre étude que « *seul un tiers environ des entreprises au Royaume-Uni réalise une estimation de l'impact financier potentiel de cyber-attaques; et que 60% de sociétés d'Europe continentale n'ont jamais estimé l'impact financier d'un scénario de cyber-perte*[127]. »

Figure 3: Enquêtes sur les approches de gestion du cyber-risque utilisées par les entreprises

Question: Votre société développe-t-elle un modèle quantitatif pour évaluer et gérer le cyber-risque?



Source : *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey*, SANS Institute, 2016.

[127] Marsh Report: «UK Cyber Risk Survey, Report, September 2016 et Continental European Cyber RiskSurvey,Report, Octobre 2016.

On peut remarquer que seul 25% des entreprises ont un modèle de quantification du risque cyber détaillé leur permettant de connaitre l'impact financier que peut causer une attaque cyber aux sein de l'entreprise, tandis que près de 60% n'ont pas encore une stratégie claire élaborée au sein de l'entreprise pour quantifier clairement le risque cyber.

Les approches quantitatives permettent de mieux appréhender l'exposition de l'entreprise au risque cyber et d'en déduire une estimation de l'impact financier en cas de réalisation du scénario. Ce type de méthode est aussi utilisé par le marché de l'assurance pour évaluer leur perte maximale en cas de sinistre. A travers cet outil, les assureurs peuvent identifier leurs cumuls et les risques corrélés, tout en mettant à l'épreuve leurs portefeuilles à des stress tests pour une série de cyber pertes. L'objectif serait de déterminer un niveau maximal de perte probable et à mieux appréhender leur risque agrégé, suite à une attaque cyber. C'est ce qu'on peut constater dans le marché de l'assurance Britannique, où le Lloyd's of London avait, en 2015, demandé à ses collaborateurs de soumettre des scénarios de cyber attaque extrême à une série de stress tests, et de faire une estimation de leur exposition agrégée potentielle dans les différents scénarios[128].

Le constat est le même particulièrement dans le secteur maritime, où le risque cyber est, pendant longtemps marginalisé, minimisé. Il a fallu une répétition d'attaques cyber, de plus en plus violentes, tant financièrement, que matériellement pour adopter une cyber-geste barrière.

Les compagnies maritimes investissent de plus en plus dans les tests proactifs de simulation d'attaques cyber avec des hackers professionnels connus le plus souvent sous le nom de hackers éthiques. En Europe le phénomène n'est pas totalement connu. Par contre, aux Etats-Unis, il n'est pas rare que des hackers autodidactes estampillés « *White Hat* » et résolvant des bugs via des plateformes de bugs bounty, soient à la suite embauchés par les entreprises victimes de ces bugs. La pratique semble malsaine mais elle permet au moins de réduire les risques d'attaques cyber et les éventuelles pertes financières ou atteinte à

[128]Cyber-attack:managing catastrophe-risk and exposures»,Lloyds.com,9novembre2015.

l'image. En France, il existe des hackers éthiques. Ce sont des experts en SI à la base, qui peuvent être formés à la suite en cybercriminalité.

La question qui se pose, au vu du retard constaté dans la prise de conscience du risque cyber par le secteur maritime, est : ne devrait-on pas adopter une solution de tests anti-phishing réguliers? Un test de résistance des SI pourrait aider les compagnies maritimes à mieux sécuriser leur système informatique et à conforter les assureurs dans leur volonté de développer le marché de la cyberassurance. Ainsi, les assureurs ont besoin de se rassurer du niveau de sécurité des SI, raison pour laquelle il est important pour eux de vérifier la vulnérabilité des systèmes, d'effectuer des tests d'intrusion interne et externe voire même accompagner les compagnies maritimes dans la mise en place de stratégies de gestion de crise. Sans cela, l'investissement sur le marché de l'assurance cyber demeurera très limité. Néanmoins, le marché de l'assurance cyber est en plein essor et nécessite une augmentation des capacités.

SECTION 2: AUGMENTER LA CAPACITÉ DU MARCHÉ

Aujourd'hui le marché de l'assurance cyber est en plein essor. Pourtant les experts estiment que sa capacité est encore très modeste. En effet, la potentialité du marché n'étant plus à démontrer, il faut donc que les assureurs augmentent leurs moyens financiers et humains pour pouvoir couvrir le risque cyber de manière plus large (**Sous-section 1**). Toutefois, il sera difficile d'absorber tout le potentiel du marché dans les années à venir, c'est pourquoi une diversification des intervenants sur le marché pourrait augmenter les chances de pérennité du marché (**Sous-section 2).**

Sous-section 1: Augmenter les moyens financiers et humains

La pérennité du marché cyber dépend fortement de la capacité des acteurs économiques. Mais aujourd'hui, on constate que la capacité financière des assureurs est en dessous de la réalité du risque (A). En effet cette capacité contrôlée, démontre carrément le manque d'appétit des assureurs pour le risque cyber. Mais pour avoir le monopole sur ce marché très prometteur, les assureurs doivent étendre leur capacité, en recrutant davantage

de spécialistes en cyber risque (B) et si nécessaire de développer un département cyber au sein de la compagnie (C).

A) Une capacité toujours en dessous de la réalité du risque

Depuis quelques années on constate une croissance des produits assurantiels couvrant les risques cyber et témoignant d'une meilleure prise en charge de ceux-ci au niveau national et international. Toutefois, le marché de la cyberassurance demeure toujours, à ce jour, limité.

Dans une étude menée par March, en avril 2014, on apprend que les assureurs ont une capacité globale mobilisable estimée à 500-700 millions de dollars[129] pour un contrat. Dans le rapport du Club des juriste publié en 2018, on observe que « *la capacité délivré par certains assureurs est de l'ordre de 75 à 100 millions de dollars, et la capacité moyenne par assureurs serait d'environ de 25 millions de dollars*[130] *»*. Ces chiffres concernent la quasi-totalité des secteurs d'activité y compris le secteur maritime. Cette capacité financière, modeste, est très loin des estimations de la sinistralité constatée, qui s'évaluent à hauteur de milliards de dollars. Ces chiffres n'ont pas trop évolué jusqu'à présent.

Il est à noter, par ailleurs, que la capacité théorique et celle réellement déployée par les assureurs fluctuent considérablement en fonction de la qualité du risque et de la sensibilité de l'activité. Nous savons que le secteur maritime est très sensible aux risques cyber en raison de sa dépendance accrue à l'internet, comme la plupart des secteurs d'ailleurs. Mais la particularité du monde maritime est qu'il s'agit d'un secteur qui pèse lourd dans l'économie mondiale. Et il suffit d'une attaque cyber touchant un géant maritime pour paralyser une grande partie de l'activité et par conséquent impacter l'économie. C'est la raison pour laquelle les assureurs, conscients de l'impact financier que peut causer une attaque cyber, n'hésiteront pas parfois à « *décliner les risques s'il considèrent que le niveau de sécurité développé par les entreprises n'est pas en*

[129] March, Benchmarking trends: Interest in cyber insurance continues to climb, avril 2014.
[130] « Assurer le risque cyber », Club des juristes, Rapport, Tome I, janvier 2019.

adéquation avec les enjeux informatiques de leurs activités », souligne Ezechiel Symenouh[131].

A l'heure actuelle, la question de l'assurabilité du risque cyber oppose toujours les acteurs. En effet, si les uns se mettent en garde sur un « territoire inexploré » et restent sceptiques sur la capacité de l'industrie à développer le marché ; les autres se manifestent plus optimistes, plus confiants au développement du marché à l'image de Bengtvon tell[132] qui pense qu'avec la nouvelle réglementation mise en place par les gouvernements, la demande va s'accélérer. « *Nous sommes actifs sur le cyber depuis dix ans aux Etats-Unis et depuis plusieurs années en Europe, alors que d'autres disent encore qu'il s'agit d'un risque inassurable…* » déclare-il. Toutefois, il s'agit d'une confiance relative et comme disait Didier Parsoire[133] « *Nous montrons un appétit contrôlé et déployons notre capacité au fur et à mesure que notre compréhension du risque progresse.* » Cela laisse paraître l'intérêt que porte l'industrie au marché de l'assurance cyber, mais reste prudente face à un risque évolutif et polymorphe, et donc compliqué à appréhender.

Il est vrai que le marché de l'assurance cyber a un très haut potentiel. Mais les assureurs doivent être en mesure de développer des produits qui correspondent à la demande tout en ayant un prix bien identifié, qu'ils se soient débarrassés des couvertures « silencieuses » et qu'aussi la prime attachée à la couverture du contrat soit identifiée. Ainsi, ils éviteront les conséquences d'un événement cyber de type catastrophe. Cependant, à l'heure de la sinistralité, il serait difficile de représenter le pire cas de figure si ce n'est que les quelques études élaborées par certains organismes sur l'impact d'une attaque cyber sur l'économie mondiale et le marché de l'assurance *(cf Scénario Shen Attack).*

[131] Chargé de comptes Cyber Risques, Practice Leader chez Willis Towers Watson.
[132] Responsable du cyber pour l'Europe et l'Amérique latine chez Munich Re.
[133] Responsable de la souscription pour les solutions cyber chez Scor.

B) Renforcer l'effectif spécialisé

Dans un contexte de dépendance numérique et de contrainte réglementaire, les assureurs doivent au-delà de la proposition de produits assurantiels, jouer un rôle de conseiller et de gestionnaire des incidents cyber. Dans l'étude menée par le club des juristes, publiée en janvier 2018, la commission ad hoc cyber Risk propos souligne que « *les assureurs sont appelés à assumer, en plus de la couverture d'assurance des incidents cyber, un rôle élargi d'accompagnement des entreprises*[134]. » Pour eux, les assureurs doivent avoir pour mission non seulement la couverture des risques, mais aussi l'accompagnement les entreprises dans la prise en charge des risques cyber. Ce rôle d'accompagnement s'analyse à travers trois axes:

- *l'information sur les développements de la menace et la veille juridique;*
- *l'analyse de risque et le conseil en prévention et mitigation des risques afin de réduire la vulnérabilité aux incidents cyber pendant la période de couverture;*
- *le suivi de la gestion de crise et l'analyse de ses impacts financiers et opérationnels afin de réduire l'impact des incidents cyber*[135].

Cela requiert une expertise suffisante que les assureurs peinent à mettre en place, en raison de son coût mais aussi du fait que le marché de l'assurance cyber soit encore en maturité et qu'il serait prématuré de recruter des salariés experts en la matière. Tout de même, l'assureur doit anticiper sur la question pour « *monter en compétence et être en mesure de dialoguer avec ses clients et de les conseiller, non seulement dans le choix de la solution assurantielle la mieux adaptée, mais aussi dans leur gestion du risque*[136]. » Donc le besoin de ressources humaines spécialisées est nécessaire pour le développement du marché.

De plus, le marché de la cyberassurance se développe à un rythme soutenu. En effet, selon les données de Munich Re, « le marché est évalué à 3,5 milliards USD à fin

[134] Club des juristes, Assurer le risque cyber, Rapport, janvier 2018, p79
[135] *Ibid*
[136] Gaspard FEREY Nicolas GROROD Simon LEGUIL, L'assurance des risques cyber, Mines ParisTech, 2017, p54

2018[137] ». Toutefois, on se demande si la crise sanitaire liée à la Covid-19 ne va pas impacter le marché de la cyberassurance. On constate tout de même une augmentation considérable de la cyber menace entre janvier et avril 2020, selon le dernier rapport de INTERPOL[138]. Mais quoi qu'il en soit, le marché de la cyberassurance est très prometteur et devra atteindre, toujours selon le réassureur allemand, « 20 milliards USD de primes à l'horizon 2025 ».

L'importance d'avoir une expertise suffisante se justifie par le fait qu'elle permet à l'assureur, de mettre en place, avec l'assuré, un cadre d'analyse pré-incident et un cadre d'analyse durant et après l'incident. Le cadre d'analyse pré-incident permet d'identifier l'ensemble des actifs gérés, y compris les données. Cela permet de déterminer la surface d'attaque[139], de préparer l'entreprise à limiter les risques de cybersécurité. Le cadre d'analyse durant et après l'incident, quant à lui, permet de détecter les signaux et de réduire l'impact de l'incident. L'objectif est de rendre le service rapidement opérationnel à l'assuré, tout en préservant les éléments de preuve et en recherchant les responsabilités et l'origine des attaques[140].

Il est, certes vrai, qu'aujourd'hui les assureurs naviguent dans des eaux troubles pour assurer le risque cyber, mais, au lieu de se limiter à renforcer l'effectif spécialisé, il serait plus intéressant de développer un département cyber au sein de la compagnie pour une réaction plus rapide.

C) Développer un département « cyber »

La plupart des compagnies d'assurance ne disposent pas de département spécialisé pour les questions de cyber. Comme nous l'avons précédemment démontré, le risque cyber est un risque entouré de beaucoup d'inconnus, ce qui fait que les assureurs, à l'heure actuelle, y consacrent très peu d'énergie. Mais pour un marché aussi prometteur, avec 2 milliards de dollars de prime rien qu'aux Etats-Unis en 2018, et 3,5 milliards de dollars

[137] https://www.atlas-mag.net/article/le-marche-de-la-cyberassurance-en-2019 .
[138] INTERPOL, « Cybercrime : Covid-19 impact », Août 2020.
[139] « Cyber-risques: Enjeux, approches et gouvernance », IFACI, Juin 2018, p8.
[140] https://cybex-assistance.com/

dans le monde, les assureurs s'y intéressent de plus en plus. Cependant, une bonne compréhension du risque cyber nécessite des compétences cyber particulières. En effet, les assureurs ne disposent pas d'une expertise cyber suffisante, leur permettant de pouvoir communiquer et de tenir un dialogue constructif avec les clients. Or, dans le cadre du risque cyber, la maitrise de tous les aspects du risque semble cruciale pour ne pas s'aventurer dans du « bricolage assurantielle », pour un risque aussi complexe et dont les conséquences peuvent être ingérables ou difficilement supportables. Les assureurs reconnaissent, d'ailleurs, une absence de ressource humaine spécialisée et par conséquent, une incapacité à communiquer avec les assurés et à fortiori de développer un marché de cyberassurance efficace.

Il faut noter que cette absence de département « cyber » au sein des compagnies d'assurance, est due à une « *difficulté à recruter du personnel qualifié à laquelle s'ajoute celle de les faire travailler efficacement en collaboration avec les métiers traditionnels de l'assurance*[141]. » Cette difficulté s'explique par le fait que les experts en la matière sont souvent des techniciens, attachés à l'innovation et à l'optimisation des procédés qui revendiquent une évolution exponentielle dans leur domaine. Ce qui n'est pas toujours compatible avec les métiers traditionnels de l'assurance qui sont souvent caractérisés par un rythme plus mesuré, plus précautionneux et très méthodique. Cet environnement hiérarchique et standardisé ne facilite pas la coordination efficiente et efficace de tous les intervenants. Et donc, créer un département « cyber » au sein de la compagnie ou de la mutuelle peut paraitre problématique dans la mesure où elles peinent à constituer une équipe et à la garder de manière permanente. La plupart du temps, elles font recours à des prestataires Cloud ou à des sociétés d'assurance spécialisées en la matière. Ce qui rend la couverture du risque plus chère et donc moins appétissante pour les assureurs.

Il est important de souligner pour la pérennité du marché cyber, il serait plus intéressant pour les compagnies d'assurance de créer un département dédié à l'assurance cyber avec des salariés formés dans ce domaine.

[141] Gaspard FEREY Nicolas GROROD Simon LEGUIL, L'assurance des risques cyber, Mines ParisTech, 2017, p54

Sous-section 2: Diversifier les intervenants sur le marché cyber

La diversification des intervenants sur le marché cyber permettrait aux assureurs d'atténuer le poids du risque cyber (A) mais aussi et surtout de partager le risque avec les fournisseurs de capitaux (B).

A) L'atténuation du risque pour l'assureur

1) L'intervention de la réassurance traditionnelle

Le risque cyber rend la compréhension des couvertures complexe en raison de son caractère évolutif et polymorphe. Assureurs et réassureurs tentent de concevoir des techniques leur permettant de mieux appréhender la conception de ce risque. Les assureurs se tournent le plus souvent vers les réassureurs pour atténuer le poids du risque cyber. A ce titre, « *la réassurance constitue un outil de premier plan pour un assureur dans la gestion de ses risques et notamment pour pénétrer le marché*[142] . » Ce qui veut dire que les assureurs doivent renforcer leur lien avec les réassureurs afin de maitriser et d'augmenter la capacité du marché de l'assurance cyber. Toutefois, il est à noter que les réassureurs comme les assureurs ne disposent toujours pas de toutes les données nécessaires dans la prise en charge du risque.

La première difficulté pour les réassureurs réside dans la connaissance de l'exposition au risque des cédants. En effet, la plupart des polices proposées par les assureurs répondent à des besoins de couverture tant en dommage qu'en responsabilité civile. Il n'est pas rare de voir certaines de ces garanties couvertes de manière implicite par des polices traditionnelles.

Les protections en réassurance peuvent être proposées via des montages en « facultative », c'est à dire que les assureurs proposent leurs risques un par un aux réassureurs, ou lorsqu'il s'agit de couvertures affirmatives, par la mise en place de traités dédiés couvrant des risques cyber de l'assureur[143].

En principe, le réassureur propose des couvertures du risque cyber proportionnelles. Cela veut dire qu'il reçoit du cédant (assureur), une fraction de prime correspondant au

[142] « Emergence du besoin en cyber assurance », Compte rendu du groupe de travail Cyber-risques, Institut des actuaires, 2017, p37.
[143] Aurélie Abadie, « Cyber réassurance, mode d'emploi », https://www.argusdelassurance.com/les-assureurs/cyber-reassurance-mode-d-emploi.151870 , 05/09/2019.

risque cédé et supporte alors une proportion du sinistre correspondant à la part cédée. Le réassureur n'intervient, alors que lorsque l'assureur direct a couvert sa fraction proposée du risque. Il existe deux modalités de réassurance proportionnelle: la réassurance proportionnelle en excédant du risque et la réassurance proportionnelle en quote-part. Dans la pratique, la seconde est la modalité la plus utilisée dans laquelle la part du sinistre à la charge du réassureur est exprimée en pourcentage de la prime cédée.

Dans le cadre du risque cyber, cette structure est difficile à mettre en place en raison de nombreuses incertitudes qui règnent encore sur ce risque. Mais, avec une connaissance plus large du risque, les acteurs de l'assurance maritime doivent pouvoir « *remonter la limite et d'offrir une couverture qui correspond aux besoins du marché*[144] », c'est l'un des plus grands défis que le monde de l'assurance maritime doit relever.

En outre, on constate depuis quelques années, le développement d'une réassurance non proportionnelle. En effet, le réassureur n'intervient que pour les sinistres qui dépassent un certain montant prévu au contrat. Dans ce type de garantie, l'engagement du réassureur est restreint par des clauses du traité.

Il est certes indéniable que le renforcement des capacités du marché ne peut se faire sans la participation des réassureurs, mais le rapprochement des assureurs aux acteurs de la cyber-sécurité est aussi un défi que les assureurs doivent relever.

2) Le rapprochement entre assureurs et acteurs de la cybersécurité

La menace cyber qui pèse aujourd'hui sur le secteur maritime oblige certains acteurs du secteur à transférer ce risque évolutif et complexe vers le marché de l'assurance. L'assurance est un moyen efficace que les compagnies maritimes peuvent utiliser pour se protéger contre les pertes d'une attaque cyber ou qu'une erreur non intentionnelle de manipulation peut générer[145]. C'est donc une nécessité vitale pour le secteur maritime. Cependant, au vu de la demande globale de couverture du risque cyber, les assureurs doivent non seulement adopter une politique de renforcement des capacités, mais aussi

[144] Op.Cit.p15.

[145] « Assurer le risque cyber: quels enjeux?, Fédération Française de l'Assurance, https://www.ffa-assurance.fr/actualites/assurer-le-risque-cyber-quels-enjeux , 18/01/2018.

essayer de se rapprocher aux acteurs de la cyber-sécurité qui, dans l'immédiat, semblent connaître le mieux ce nouveau risque.

Dans la pratique, des partenariats ont vu le jour dans cette lancée, à l'image de Axa et Airbus ou Allianz et Thalès. Ces partenariats s'avèrent particulièrement attirants dans la mesure où, ils permettent de proposer des « *contrats d'assurance qui couvrent les dommages subis suite à une cyber-attaque et un accompagnement en ingénierie sur mesure pour aider les entreprises à se protéger contre les cyber-risques*[146]. » Cela a un double avantage: d'une part il permet une prise en charge du risque en binôme, avec plus de données à disposition. En effet, les assureurs et les acteurs de la cyber-sécurité peuvent élaborer une approche globale du risque cyber et avancer tous les paramètres. Cela faciliterait, non seulement la quantification du risque, mais aussi l'évaluation de la cyber-exposition. D'autre part, l'accompagnement en ingénierie renforcerait également la confiance des entreprises maritimes dans le partage d'informations.

Dans un terrain encore méconnu des assureurs, ce rapprochement peut être un défi crucial dans le monopole du marché de l'assurance cyber. Et à l'image des compagnies maritimes, l'assurance cyber donne une bonne réputation à l'entreprise. D'autant plus que « *la mise en place de polices de cyberassurance impose naturellement avec plus de rigueur des dispositifs de contrôle et facilite les investissements en matière de surveillance des systèmes*. » selon PwC. Il est donc important pour les assureurs d'avoir une vision plus large du marché avec les partenaires afin de développer des offres de cyberassurance plus adaptées aux besoins du secteur maritime. Ce rapprochement peut également donner la possibilité aux assureurs de s'allier dans la création d'offres nouvelles, mais aussi dans leur distribution, avec des fournisseurs de solutions de cybersécurité. Dans une étude publiée en janvier 2016, par PwC, on apprend qu'il est même possible de voir dans le futur des « *rapprochements de nature capitalistiques entre grandes compagnies d'assurance et géants de la cyber-sécurité*[147] », bien évidemment, lorsque le cyber risque deviendra la pierre angulaire de l'ensemble des offres d'assurance. Mais, il faut au préalable disposer de tous les acquis nécessaires pour quantifier et modéliser les cyber risques. Ce

[146] « Le marché de la cyber-assurance: la révolution commence maintenant », PwC, janvier 2016
[147] Op. cit. p 17.

rapprochement entre les assureurs et les acteurs de la cybersécurité s'observe aussi dans des secteurs comme l'automobile ou le secteur du bâtiment. Dans l'industrie de l'assurance, le rapprochement doit encore se structurer mais on constate que les assureurs migrent de plus en plus vers les marchés financiers.

B) Le partage du risque avec les fournisseurs de capitaux

1) Le transfert du risque cyber vers les marchés financiers : La titrisation du risque cyber

Il est clair que les assureurs ne peuvent pas absorber toutes les pertes liées au risque cyber. Il serait alors nécessaire de transférer une partie du risque aux marchés de capitaux pour faire en sorte que les garanties ou limites proposées soient plus élevées, afin de rendre la couverture du risque cyber plus facile à souscrire et les risques plus largement répartis entre les intervenants. La diversification des acteurs du marché est cruciale pour le développement de celui-ci, car comme nous l'avons démontré tantôt, le risque cyber est un risque tellement grand qu'il serait difficile à absorber seul. L'intervention ou la participation des marchés financiers dans la maitrise du risque cyber permettra aux assureurs et réassureurs de ne pas trop s'exposer au cyber. Etant donné qu'au-delà d'un certain stade, l'ampleur potentielle des pertes de certaines attaques cyber pourrait dépasser la capacité de couverture du secteur privé de l'assurance et de la réassurance[148].

L'élargissement de la capacité générale d'absorption des pertes liées aux risques cyber peut se faire avec la création de véhicules d'investissement permettant de faire supporter une partie des expositions par les investisseurs sur les marché financiers[149]. Cette approche pourrait, en effet, permettre de pallier les déficiences du marché traditionnel avec la titrisation du risque cyber ; à l'instar de ce qui existe déjà pour les risques de catastrophes naturelles, qui a donné naissances aux obligations de catastrophes *(Cat Bonds).* Ces « *Cat Bonds* » permettent de couvrir les risques de grande ampleur que ni les assureurs, ni les réassureurs ne sont en mesure de gérer. La plupart des *Cat Bonds* sont

[148] « Réassurance: Et si le risque cyber bénéficiait d'un « filet de sécurité » de l'Etat?,MarionaVivar, 2 mars 2017.
https://www.newsassurancespro.com/reassurance-certains-risques-cyber-beneficiaient-de-garantie-detat/0169314696

[149] « Cyber: Comment venir à bout d'un risque complexe? », SwissRe Institute, n°1, 2017, p33.

affectés aux risques de dommages aux biens. Mais, depuis quelques temps, on constate une généralisation de ces titres aux autres branches de l'assurance notamment les risques accidents, vie ou santé.

Ce transfert de risque aux marchés financiers augmenterait non seulement la capacité du marché, avec le recours aux fonds de titrisation d'assurance plus connu sous le nom de « *Insurance-Linked Securities* » (ILS), mais donnerait aussi une occasion aux assureurs et réassureurs de proposer des solutions assurantielles plus adaptées et plus larges pour viabiliser le marché cyber. C'est d'ailleurs ce que souligne Alexandre Hassler[150] qui estime qu' *« une solution pour résoudre la question du manque de capacité pourrait être d'émettre sur les marchés financiers des titres pour couvrir des événements cyber, des sortes de cyber bonds*[151].» Concrètement, les « *Cyber bonds* » peuvent permettre aux assureurs et réassureurs qui veulent titriser une partie de leur portefeuille cyber auprès des investisseurs, d'émettre des titres pour couvrir les risques cyber. Ce système augmenterait considérablement l'aptitude du marché d'assurance à fournir des capacités suffisantes et liquides, même dans les scénarios les plus extrêmes d'évènements cyber.

La pérennité du marché de l'assurance cyber réside dans le partage du risque entre acteurs de la vie économique. Il va donc falloir que les assureurs et réassureurs reconnaissent leur incapacité à faire face, seuls, au risque cyber. Il leur faudra développer aussi des accords proportionnels en vertu desquels les cyber-risques pourront être partagés entre investisseurs et souscripteurs d'assurance professionnels (au lieu des habituelles structures en excédent de sinistres) favorisant ainsi l'expansion du marché des ILS[152].

2) Les freins au développement d'un marché alternatif de transfert du risque

Nous savons maintenant que le marché de l'assurance ne peut, à lui seul, absorber toutes les pertes causées par un incident cyber en raison de son caractère potentiellement systémique. Son transfert vers les marchés financiers en vue de l'obtention de titres pour couvrir des événements cyber est alors nécessaire pour la pérennité du marché. Mais, si la

[150] Actuaire certifié, courtier en assurance et réassurance, Lyon Re.
[151] « Cyberassurance: digérer la part de risque, 20 septembre 2018. https://www.institutdesactuaires.com/magazine/article/cyberassurance-digerer-la-part-de-risques/2549
[152] « Cyber: Comment venir à bout d'un risque complexe? », SwissRe Institute, n°1, 2017, p33.

titrisation du risque cyber peut être un enjeu capital pour la viabilité du marché de l'assurance cyber, il serait indispensable pour l'industrie de l'assurance, d'apporter une garantie de sa rentabilité pour gagner la confiance des investisseurs. Dans la pratique, il est vrai que les ILS ne sont pas encore totalement expérimentés dans le cadre des risques cyber, mais nous avons précédemment démontré dans la Partie I, qu'une attaque cyber peut avoir un impact abyssal sur le cours de l'action de la victime et que cela pourrait aussi toucher la valeur des investissements sur les marchés des actions et des obligations[153].

Face à des investisseurs dubitatifs sur l'essor du marché de l'assurance cyber, les assureurs doivent pouvoir les convaincre des bénéficies en matière de diversification offertes par les cyber-risques. Toutefois, il existe quelques obstacles en dehors de l'absence de données et des problèmes de modélisation, que les acteurs doivent surmonter afin d'établir des accords proportionnels avec les investisseurs pour le risque cyber.

L'étude de Swiss Re consacré au risque cyber soulève deux facteurs susceptible de freins l'essor d'ILS pour cyber-risque. D'une part, les investisseurs souhaiteront avoir davantage la certitude que les rendements des titres liés aux cyber-risques sont réellement non corrélés à d'autres classes d'actifs[154]. La peur des investisseurs est de faire face à un événement cyber qui aurait impacté tout le marché du crédit et des actions. Ils veulent se rassurer de la rentabilité avant d'investir sur ce marché encore à maturité. D'autres parts, il y a une base de risque important. En effet, les sponsors préfèrent une garantie pour tous les scénarios possibles afin de compenser la totalité des pertes encourues. Ainsi, selon SwissRe « *les investisseurs demandent des titres où le paiement est déclenché par des paramètres bien définis et observables, qui ont l'avantage de réduire le risque d'anti-sélection et le risque moral, […] et de baisser leur coûts d'évaluation des résultats financiers et de souscription des compagnies* ». A ce titre, un problème de préférence semble se poser. Il faut donc essayer de trouver un équilibre sur les préférences des uns et des autres pour mettre efficacement en place, un marché de transfert des risques pouvant pérenniser le marché de l'assurance cyber qui est déjà redoutable.

[153] Op. cit. p16.
[154] Op. cit. p16

Toutefois, malgré les nombreuses difficultés constatées dans la prise en charge du risque cyber, tant dans l'approche technique que dans la capacité très modeste du marché, l'industrie de l'assurance reconnait que le cyber risque est un marché à très haut potentiel et la conquête de ce nouveau marché nécessite des solutions et des stratégies assurantielles adaptées.

CHAPITRE 2. DES SOLUTIONS ET STRATÉGIES ASSURANTIELLES ADAPTÉES

La plupart des assureurs ayant acceptée de couvrir le risque cyber le font souvent par des offres de garantie spéciales complémentaires. Comme nous l'avons démonté dans la première partie, les polices traditionnelles exclus les risques cyber de leur couverture. Mais face à l'urgence s'est vu émerger des solutions (**Section 1**). En effet les assureurs essayent de s'adapter en proposant une cyberassurance qui permet aux entreprises de minimiser l'impact financier suite à un incident cyber ou coordonnant le risque cyber avec les risques classiques. Mais force est de constater que les solutions des assureurs et réassureurs peuvent ne pas suffire pour les risques cyber de grande ampleur et que des solutions émanant d'acteurs externes au marché peuvent être nécessaire (**Section 2**).

SECTION I. L'ÉMERGENCE DES SOLUTIONS EXISTANTES

Les compagnies maritimes ont besoin des assureurs pour préparer leur cyber-résilience. A ce titre la cyberassurance peut être un outil fondamental permettant aux acteurs du monde maritime de se prémunir contre le risque cyber (**Sous-section 1**). Pourtant on remarque que la plupart des assureurs ont tendance à coordonner le risque cyber aux autres branches de l'assurance (Sous-section 2).

Sous-section 1. La cyberassurance: une source d'innovation majeure de résilience face au risque cyber

Il faut le dire, la cyberassurance est la solution principale pour les compagnies maritimes de se protéger contre le cyber risque. Il est vrai que les produits de couverture cyber sont nouveaux sur le marché mais on note une augmentation de la demande de cyber assurance. Cette augmentation de la demande montre le rôle clé de la cyberassurance pour les entreprises (A). Ainsi le marché de l'assurance cyber commence à proposer des polices cyber type mieux adaptées aux besoins des clients (B).

A) Le rôle clé de la cyberassurance

C'est au début des années 2000, qu'est né, aux Etats-Unis, les premiers contrats d'assurance cyber « purs ». Historiquement, les Etats unis font partie des premiers pays à se pencher sur la question du transfert du risque cyber au marché de l'assurance. Maintenant que la question de la probabilité d'occurrence ou de l'impact au sein de la compagnie maritime ne se pose plus; les entreprises étaient face à un risque dont le seul moyen de s'en préserver est de le lisser par voie de transfert au marché de l'assurance. L'idée est de permettre aux compagnies maritimes de bénéficier de l'intervention très rapide des assureurs par le biais de leurs experts spécialisés. Cette intervention permettra de déterminer l'origine de l'attaque, de la contenir et de définir les processus à activer pour assurer la disponibilité des ressources informatiques et la continuité des activités critiques. Cette solution assurantielle proposée par les assureurs engendre une approche sur mesure du risque. Les assureurs maritimes ont un rôle primordial à jouer dans le développement de la cyber-résilience des entreprises maritimes. C'est ce qu'on peut retenir du communiqué de presse[155] du Président de la société Bessé[156] lorsqu'il souligne que « *nous intervenons au quotidien dans la gestion de la crise pour orienter et accompagner les prises de décision d'ordre stratégique.[…] Nous avons un vrai rôle à jouer aussi bien dans l'indemnisation du sinistre que dans la diffusion des bonnes pratiques et le développement de la cyber-résilience… ».* C'est une approche proactive du risque cyber qui doit être adapté par tous les acteurs de l'industrie maritime. Dans un vrai sens de l'anticipation et d'une approche volontariste de la révolution 4.0, cela leur permettrait de réduire le champ d'attaque des pirates informatiques.

Partant de là, on peut dire que la cyberassurance est en plein essor ; et même si elle est encore balbutiante, elle pourrait tirer tout l'écosystème vers le haut. Aujourd'hui le marché mondial de l'assurance cyber est estimé à plus de 7 milliards et ce chiffre devra doubler à l'horizon 2022[157]. Certains acteurs proposent même une cyberassurance obligatoire comme dans l'assurance automobile. Mais cette idée est pour le moment

[155] Salon International Pacific Sydney, Communiqué de presse, Octobre 2019
[156] Bessé, Leader Français dans le conseil en assurance des risques liés aux industries de la Défense.
[157] Global Cyber InsuranceMarket Report, AlliedMarketResearch,

immature, du fait qu'il est déjà problématique de faire prendre conscience à l'ensemble des acteurs du secteur maritime de leur vulnérabilité face au risque cyber et des conséquences qu'une éventuelle attaque cyber peut engendre dans la compagnie. Il va falloir que tous que tous les acteurs de l'industrie soient conscients du risque et de sa dangerosité sur le plan financier, et de les encourager à souscrire une police cyberassurance. Dans le récent rapport de Hiscox, nous avons pu observer qu'en 2019, seul 41% des répondants[158] ont confirmé que leur entreprise avait souscrit une cyberassurance, contre 33% en 2018 et 40% en 2017. (**Voir Annexe 3**)

La cyberassurance est certes un moyen imparable pour les compagnies maritimes, mais son développement est à devenir. Cela est dû aux manques d'informations des assurés. Dans le rapport publié par Hiscox, la plupart des entreprises ayants répondu « *pas certains de savoir ce qu'est une cyber assurance* » sont des PME. Pourtant, ils sont les plus exposés au risque cyber, qui au-delà de sa complexité, est potentiellement systémique. Dans le monde maritime un géant peut être victime d'attaque et survivre à cette attaque, l'image de Maersk, en 2017, mais il serait difficile pour une PME du secteur maritime de résister à une attaque cyber. L'impact serait trop important pour se relever suite à un incident cyber. Il est donc primordial voir même nécessaire pour ces PME de prendre conscience du risque et de souscrire une police assurance-cyber si elles ne veulent pas disparaître. Mais reste à savoir si les PME ont les capacités financières et technologiques de générer des dépenses dédiées à la cybersécurité.

Sur le marché français, les assureurs peinent à modéliser et qualifier les risques cyber par secteur d'activité, ce qui ne favorise pas la mise en place de produit cyber lisible[159]. Du côté des entreprises, cette difficulté à modéliser et à quantifier est plus liée aux offres coûteuses et aux solutions non adaptés à eux[160]. En ce qui concerne particulièrement le secteur maritime, les assureurs doivent se concentrer sur la mise en

[158] Les répondants sont issus presque de tous les secteurs d'activité de 7 pays différents: Allemagne, Espagne, Etat-Unis, France, Royaume-Uni, Belgique, Pays-Bas. 39%(Petites entreprises); 16% (Moyennes entreprises); 16% (Grandes entreprises); 28% (très grandes entreprises).
[159] « Comment « débloquer » le marché de l'assurance cyber en France? », Telecom Paris Tech, Alumni, Livre Blanc, Juin 2017, p11.
[160] *Ibid, p11*.

place d'une cyberassurance adaptée aux besoins du secteur. À l'image de ce que Willis Tower Watson effectue pour le secteur de l'aviation. Il propose un nouveau produit adapté au secteur de l'aviation (*CyFly*). Ce produit comprend des innovations spécifiques au marché des compagnies aériennes. Il contient des extensions de pertes d'exploitation à des tiers. En effet les compagnies aériennes s'appuient sur un grand nombre de service de tiers pour assurer la continuité des activités[161].

Nous savons que le secteur maritime est en retard par rapport à d'autres secteurs, sur le risque cyber; mais il est du ressort des assureurs, de développer des polices cyber types plus adaptées aux besoins des acteurs du secteur maritime.

B) Le développement des polices cyber type

1) L'Augmentation des souscriptions cyber

Le potentiel du marché de l'assurance cyber fait que la plupart des compagnies d'assurance adoptent leur produit en fonction de l'évolution du marché. En principe, les incidents cyber sont souvent exclus des polices dommages aux biens ou des responsabilités civiles professionnelles, c'est la raison pour laquelle, certains assureurs spécialisés en la matière proposent des polices types cyber pour couvrir les conséquences d'un incident cyber comme la perte d'exploitation, la restauration de données ou les atteintes à la réputation. Actuellement, les polices cyber se développement progressivement. Selon une étude de PwC, environ un tiers des entreprises américains achètent un certain type de cyber assurance[162]. Le chiffre est de 41% pour l'ensemble des entreprises ayant souscrites une police cyber dédiée en 2019. (**Voir Annexe 3**).

En France, les entreprises sont les moins nombreuses à disposer d'une couverture de cyber-risques, à égalité avec les entreprises allemandes, révèle le rapport de Hiscox sur la gestion des cyber risques de 2019. Cela montre que les entreprises françaises ne sont pas

[161] « Willis Tower Watson launchesinnovate new cyber product for global airlines » WILLIS TOWER WATSON, Press release, Avril 2017.
[162] https://www.iiis-cyber.org/2019/04/11/cyber-assurance-c-est-quoi/

encore convaincues de la nécessité de l'assurance cyber[163]. De ce fait, en France, l'assurance cyber peine à décoller, notamment parce que sur le milieu et le bas de segment ce risque reste en inclusion de nombreux contrats de multirisque dommages[164]. Par contre, les entreprises espagnoles sont les plus nombreuses à avoir souscrit une police de cyberassurance dédiée: 49% alors que la moyenne est de 41%[165]

Jusque-là, l'industrie de l'assurance faisait des efforts pour promouvoir le produit de l'assurance cyber, qui échappait aux redressements tarifaires du marché des grands risques, mais l'augmentation des cyber-attaques liée à la pandémie de Covid-19, changera probablement la donne. Il est évident que la demande de souscription va augmenter dans les prochains mois ou années. Ce qui va certainement, pousser les porteurs de risques à établir une politique de souscription plus rigoureuse qu'auparavant sur le cyber. Reste à voir comment assureurs et courtiers vont parvenir à trouver un compromis dans ce contexte de tensions tarifaires pour rendre plus attractifs ce marché en pleine expansion.

En outre les assureurs spécialisés vont maintenant plus loin en proposant par exemple des compétences en gestion de crise. Concrètement les frais pris en charges peuvent concerner par exemple les investigations, les frais engagés auprès de tout expert informatique chargé d'analyser, de limiter les effets, de mettre fin à une atteinte aux données, une atteinte à la sécurité du système informatique, une erreur humaine ou d'assistance à un incident cyber. Elle concerne également les frais de restauration ou de reconstitution des données engagés, ainsi que les frais de restauration et de reconfiguration de logiciel. En France, certains assureurs comme Cyber-Cover proposent même la prise en charge des sanctions pécuniaires légalement assurables prononcées par une autorité administrative, dû au manquement au RGPD[166].

[163] Pourtant près d'un sur cinq des entreprises françaises déclarent avoir versé une rançon (18%) après une cyber attaque, contre 6% pour l'ensemble du panel (Etats-Unis, France, Allemagne, Royaume-Uni, Belgique, Espagne, Pays-Bas).
[164] Marie Caroline Carrière « Les entreprises françaises fortement investies par la cyber sécurité », https://www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/les-entreprises-francaises-fortement-investies-par-la-cyber-securite.168449
[165] Rapport Hiscox sur la gestion des cyber-risques, 2019.
[166] https://www.cyber-cover.fr/uploads/assurance/garanties/5c59c5f9dbd91564441249.pdf

2) L'extension du champ de la couverture

Les débuts de l'assurance des cyber-risques dans le secteur maritime ont été marqués par une limitation des garanties. En effet, les premières polices d'assurance des cyber-risques ne couvraient, la plupart du temps, que les préjudices matériels, c'est à dire les dommages physiques, subis par les appareils informatiques. Mais depuis quelques années, certains assureurs diversifient leurs offres en y introduisant des garanties complémentaires. Ces garanties couvrent notamment les dommages immatériels comme la perte d'exploitation ou l'atteinte à la réputation, et une couverture des éventuels sinistres causés aux tiers. Nous savons que les assureurs, dans la peur de couverture « silencieuse », exclu les risques cyber de leurs polices, d'où la nécessité de clarifier les contrats. C'est la raison pour laquelle, la majeure partie des contrats d'assurance et de réassurance comporte une clause explicite excluant tout événement d'origine cyber. (**Voir la partie I sur la clause dite CL380**). Ceci leur permet de cantonner les cyber-risques à des polices qui leur sont spécialement dédiées[167].

Aujourd'hui, on constate que l'industrie de l'assurance veut développer le marché en innovant dans sa gamme de produit cyber. En effet, les assureurs offrent aux compagnies maritimes des polices cyber pouvant couvrir les dommages liés à un incident cyber. Ils proposent de prendre en charge les pertes d'exploitation consécutive à une cyber attaque, le paiement de rançon, l'indemnisation des pertes de données, les dommages causés aux tiers du fait de la perte de ces données, ou encore les dommages à la réputation de l'entreprise. On note une nette évolution du champ de la couverture.

Les assureurs sont partie d'une simple prise en charge des dommages matériels subis par les appareils informatiques à une couverture plus large incluant tout dommage pouvant être causé par un incident cyber.

De plus, on remarque, depuis quelques temps, que les assureurs et réassureurs proposent des couvertures pour les dommages aux corps de navire consécutifs à une cyberattaque. C'est une offre d'assurance très récente; car les polices d'assurance corps de navire, exclu, en principe les dommages consécutifs à une cyberattaque. Toutefois dans le but de sécuriser les relations entre assureur et assuré, certains assureurs proposent depuis

[167] https://www.atlas-mag.net/article/lassurance-des-cyber-risques

peu des clauses de rachat de l'exclusion, permettant ainsi de couvrir les dommages causés au navire consécutif à une cyber attaque[168].

Enfin on peut donc remarquer que le risque cyber est systématiquement exclu des contrats traditionnels, mais les assureurs et réassureurs ne cessent de proposer des produits cyber, en parallèle des polices traditionnelles afin de protéger les compagnies maritimes de tout dommages liés à une cyberattaque. Et depuis quelques années, ce produit ne cesse d'étendre son champ de couverture.

Toutefois un nombre non négligeable d'assureurs continuent d'offrir la garantie contre les risques cyber dans les polices traditionnelles. Ce qui se définit par une coordination de la police cyber aux risques qui relèvent des branches classiques de l'assurance.

Sous-section 2 . La coordination de la police cyber aux branches classiques de l'assurance

A l'heure actuelle, il n'existe pas beaucoup de compagnies d'assurance au monde, spécialisées à la couverture des cyber risques. En général, les compagnies d'assurance qui s'y investissent, l'intègrent souvent aux contrats traditionnels avec (A) ou le couvre par une extension de garantie (B).

A) L'intégration du risque cyber aux contrats traditionnels

Si la maitrise des risques dits classique semble être plus simple, il n'en est rien pour le risque cyber, qui au-delà de l'impact financier potentiellement faramineux, peut atteindre la réputation des compagnies maritimes. L'objectif pour ces derniers ne devrait pas se limiter à maitriser le risque cyber, mais d'organiser leur cyber-résilience. A ce titre, l'assurance peut jouer un rôle crucial, en accompagnant les compagnies maritimes, que ça soit en mer ou à terre, dans une politique de cybersécurité. L'assurance peut être un moyen clé de cyber-résilience, avec les polices cyber qui peuvent prendre en charge tout ou partie des pertes constatées. Mais il serait moins complexe pour les compagnies maritimes de pouvoir coordonner la police cyber aux autres branches classiques de l'assurance.

[168] Brice Ducoum, « Industrie maritime et risque cyber », https://observatoire-fic.com/industrie-maritime-et-risque-cyber-par-brice-ducoum-groupe-eyssautier/

Avant le développement de la cyberassurance, la plupart des dommages liés au risque cyber était couvert par les polices classiques. En effet le fait générateur, qu'il soit d'origine malveillant ou d'erreur humaine, ayant engendré des dommages matériels, peut être couvert par les polices traditionnelles. Cependant, la plupart du temps les dommages liés à un incident cyber sont immatériels comme la perte d'exploitation ou l'atteinte à la réputation. Il serait donc efficace si les assureurs pourraient trouver une solution assurantielle pouvant coordonner le risque cyber et les risques traditionnels. Cela permettrait sans doute de mettre en évidence une double posture dans laquelle le marché une fois posé le principe « *tout dommage matériel reste couvert par une police dommage même s'il est consécutif ou aggravé par du cyber. Les polices RC couvrent toute la RC cyber sauf exclusion. L'intersection des polices cyber est limitée aux dommages immatériels non couverts qui font suite à une attaque cyber ciblée. La police cyber vient en complément.* » Ce qui fait que la plupart des polices traditionnelles s'étendent aux dommages liés à un incident cyber. Par exemple les polices dommages aux biens peuvent couvrir les pertes d'exploitation ou les frais informatiques. C'est le cas dans la police de l'assureur FM Global [169] . Toutefois il est important de clarifier les domaines de compétences de chacun des contrats afin d'éviter pour le client de payer deux fois pour la même nature de couverture mais également afin d'éviter des recours qui risqueraient de ralentir le processus d'indemnisation[170].

En outre, les polices responsabilité professionnelles (E&O) peuvent couvrir des dommages liés à la protection juridiques, e-réputation, amendes et pénalités, protection des données. En effet, à la suite d′un incident cyber, la responsabilité du dirigeant peut être retenue, pour non prise en compte du risque. Et dans le cadre du risque cybernétique, beaucoup de compagnies maritimes, l'ignorent ou le minimisent, pensant que leurs systèmes sont infaillibles.

[169] https://www.fmglobal.fr/products-and-services/products/cyber-resilience-solutions

[170] « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance », System X, Institut de recherche Technologique, Rapport, 2016.

Actuellement, les assureurs et réassureurs travaillent également sur la conception d'un inventaire des polices traditionnelles avec les risques cyber intégrés. Ce qui permettra sans doute aux compagnies de déplacer le risque cyber vers des polices autonomes ou de mettre en place de « cyber sous-limites ». Dans une récente étude[171] menée par BESSÉ et PwC, en mars 2018, les spécialistes estiment que l'assureur « *ne saurait se limiter à la souscription d'une police cyber spécifiques sans l'avoir coordonnée avec les risques qui relèvent des branches classiques de l'assurance: dommages aux biens, responsabilité civile, automobile, maritime, transport, aviation… ».* Autrement dit il serait plus pertinent si la question de la cyberassurance était posée de manière globale avec les assurances traditionnelles. Cela nous ramène à se demander si les données ne devront pas être considérées comme un bien assuré à part entière. La question mérite une réflexion plus profonde dans la mesure où les données font parties de l'actif de l'entreprise.

En automobile, par exemples, la question s'est déjà posé, avec les véhicules autonomes, qui sont équipés d'un système de délégation de conduite supervisé à bord ou à distance. En cas d'accident la question s'est posée de savoir, comment traiter la responsabilité en fonction du niveau de défaillance? Est-ce de la faute du conducteur « superviseur » à bord ou à distance ou du fabricant?

A l'heure actuelle, des solutions innovantes sont en cours avec la loi LOM[172]. La question de la responsabilité se posera sans doute avec l'avènement des navires autonomes. Dans ce cas les conséquences d'une vulnérabilité digitale seront-elles imputables au fabricant? Et si aucune faute ou négligence du fabricant n'est décelée? Les questions sont nombreuses, mais dans tous les cas, il nous semble plus urgent, à l'heure actuelle, de se pencher sur une approche technique sur mesure, sans pour autant chercher à maitriser parfaitement le risque cyber avant d'agir.

[171] Résultats de l'enquête de BESSÉ-PwC, Les dirigeants d'ETI face à la menace cyber, mars 2018
[172] Voir https://www.legifrance.gouv.fr/affichTexte.docategorieLien=id&cidTexte=JORFTEXT000039666574&dateTexte=

B) La couverture du risque cyber par une extension de garantie

L'offre de produits cyber est en phase d'adaptation, et de nombreux assureurs dans une approche a *minima*, propose aux clients un élargissement des polices standards par des rachats d'exclusion ou des extensions de garantie cyber.

Comme souligné *supra*, le marché de l'assurance est en phase d'adaptation pour appréhender un risque de plus en plus pervasif et multiforme. C'est ce que reflètent les produits cyber. Ils combinent des garanties dommages et responsabilité pour les conséquences matérielles et immatérielles des événements cyber[173]. Ainsi le risque cyber devient un risque universel qui s'imprègne dans tous les risques connus jusque-là. De ce constat, il est évident de reconnaitre que les risques cybernétiques peuvent générer des sinistres au titre des polices ordinaires. Lors de nos recherches nous avons eu à échanger avec un acteur du secteur de l'assurance qui nous a informé que « *les assureurs les exclus généralement des polices ordinaires et offrent la possibilité aux clients de les racheter par le biais d'une garantie spéciale complémentaire.* » Tout cela, certainement, pour éviter d'une part, de faire face à une couverture « silencieuse » du risque cyber par les polices traditionnelles, et d'autre part pour pouvoir offrir une garantie cyber autonome.

Si les assureurs offrent une extension de garantie cyber, c'est parce qu'à l'heure actuelle, ils ne disposent pas de tous les éléments fondamentaux du risque. Ils jouent sur la prudence; et comme indiqué *supra*, le marché de la cyberassurance est en quête de maturité. En effet ce processus de maturation est le fruit d'une symbiose entre connaissance et maîtrise du risque par les assurés, environnement réglementaire adapté et développement de l'expertise et des produits par les assureurs et les réassureurs[174]. Toute cette fusion est nécessaire, non seulement pour les assurés, dans leur politique de cyber-résilience, mais aussi pour les assureurs, dans la proposition de produits cyber adaptés aux besoins des clients. Mais il est vrai que, la souscription pour les garanties spéciales complémentaire (cyber), bien que très variées et très attractives, sont encore très marginales. Cela est du fait d'une prise de conscience de la dangerosité du risque cyber encore insuffisante dans le secteur maritime.

[173]Sébastien HEON et Didier PARSOIRE, « la couverture du cyber-risque », extrait de la Revue d'EconomieFinancière, n° 126, p178.
[174]*Ibid, p29.*

L'industrie maritime, contrairement au secteur terrestre ou aérien, s'est tardivement préoccupé de la question des cyber risques, et par conséquent rencontre des difficultés à définir ses besoins face aux risque cyber. Mais aujourd'hui, on aperçoit de plus en plus d'assureurs proposer des polices « tous risques informatiques » énumérant les risques garantis ou prévoyant une formules « tous risques sauf » couvrant ainsi tous les événements non expressément exclus[175]. Cette couverture supplémentaire s'adapte aux évolutions du marché. A titre illustratif, on peut citer Allianz qui propose des extensions de garantie cyber[176]. Ces garanties prennent en charge le financement de tous les frais nécessaires pour identifier et comprendre l'attaque cyber, la stopper, identifier les données touchées et les restaurer. Cependant, il faut reconnaître que ces offres sont le plus souvent observé dans le terrestre. En effet dans le cadre des risques d'entreprise, dans le terrestre, une garantie « tous risques » peut être souscrite à l'exclusion des risques de guerre ou cyber. Par la suite, l'assureur peut consentir à une garantie exceptionnelle, complémentaire pour ces derniers. La situation est semblable dans le maritime, car les risques de guerre et cyber sont exclus des polices contre les risques de mer. Mais par le biais de clauses additionnelles ou de conventions spéciales, ces risques peuvent faire l'objet de rachat.

De nos discussions avec certains assureurs, nous apprenons qu'il ne serait pas facile d'assurer les risques cyber de façon autonome car il y aura des situations où la cause des sinistres serait impossible à déterminer. Dans ces cas-là, une démarche similaire à celle prévue à l'article 172-17 du code des assurances, pour les risques de guerre est nécessaire pour le risque cyber. Selon cet article « *lorsqu'il n'est pas possible d'établir si le sinistre a pour origine un risque de guerre ou un risque de mer, il est réputé résulté d'un événement de mer* ». Cela permettra d'indemniser les victimes par le biais des garanties ordinaires. Mais à l'heure actuelle, doit-on se contenter d'un simple rachat pour la couverture du risque cyber ou se concentrer sur une police cyber plus large et plus autonome?

[175] Virginie Bensoussan-Brulé, « Cyberattaques: l'assurance cyber risques », 22 mai 2017, https://www.alain-bensoussan.com/avocats/cyberattaques-assurance-cyber-risques/2015/03/11/

[176] https://www.allianz.fr/assurances-professionnels-entreprises/mon-activite/proteger-mon-entreprise-des-cyberattaques.html

En outre de nombreux autres offres d'extension de garantie spécifiques aux cyber risques sont proposées par les assureurs. En effet lorsque le contrat d'assurance traditionnel ne prévoit pas la couverture du risque cyber, les assureurs proposent, souvent à l'assuré de couvrir les dommages concernant les frais de reconstruction des informations dans l'état antérieur au sinistre, les frais supplémentaires d'exploitation et les pertes d'exploitation, en contrepartie du versement d'une prime complémentaire.

Maintenant que la nécessité de prendre en compte la menace cyber fait l'unanimité dans le secteur maritime, et que sa prise en charge ne peut être assurée sans une réglementation adaptée, et un accompagnement de bout en bout de l'industrie de l'assurance. Il est du ressort de tous les acteurs, y compris ceux externe au marché, de collaborer afin d'apporter des solutions efficaces et adaptés aux besoins du monde maritime.

SECTION II. DES PISTES DE SOLUTIONS NOUVELLES ÉMANANT D'ACTEURS EXTERNES AU MARCHÉ

Sous-section 1. L'Etat dans l'assainissement du marché cyber

Au-delà de la réglementation, les assureurs ont besoin de l'intervention de l'Etat dans l'assainissement du marché. Si les uns suggèrent la mise en place d'une plateforme contrôler par l'Etat (A), les autres demandent une garantie en dernier ressort de l'État (B).

A) La mise en place d'une plateforme d'échange informatique entre assuré et assureur

Certains spécialistes de la question recommandent que l'État joue un rôle de tiers indépendant, en mettant en place une plateforme. En écho au mémoire de G. Ferry, N. Grorod et S.Leguil sur l'assurance des risques cyber, ils proposent que les données sinistres soient mutualisées par l'Etat à travers les prestataires de sécurité, les assureurs, les assurés et la justice. Pour eux l'ensemble de ces acteurs disposent d'informations capitales mais « a*ucun acteurs n'est en mesure de cerner en globalité l'état de la menace et de ses*

conséquences avérées dans les entreprises[177] ». Cette absence de collaborations, bénéficie d'une part aux attaquants, qui profitent du temps de réaction nécessaire au partage des recommandations de sécurité. D'autre part il empêche le marché de l'assurance de se structurer sur des bases actuarielles crédibles[178]. Ainsi la mise en place d'une plateforme d'échange informatique pourrait aider les compagnies maritimes à adopter une culture du risque cyber, mais surtout permettre aux assureurs d'avoir une base de données de sinistres cyber, qui depuis longtemps fait défaut.

Cette plateforme pourrait également permettre aux compagnies maritime qui ignorent le risques cyber et les conséquences qu'il peut engendrer de connaitre les démarches à suivre et par ricochet de les mettre en relation avec des prestataires de gestion de crises et de remédiation. C'est sur cette lancée que L'ANSSI a créé un organisme de ce type dénommé GIP ACYMA (Actions contre la Cyber Malveillance[179]. Ce groupement d'intérêt public teste depuis 2016 une plateforme numérique dans la région Haut-de-France. Il a pour objet:

- *d'assister les entreprises, les administrations et les particuliers victimes d'actes de cybermalveillance*;
- *de sensibiliser aussi le public sur les enjeux de la sécurité et de la protection de la vie privée numérique en lien avec les autorités compétentes et le développement de campagne de prévention;*
- *de fournir des éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux anticiper à travers la création d'un observatoire dédié.*

En d'autres termes le GIP ACYMA a pour mission de recueillir les données sincères et diriger les entreprises sinistrées vers les prestataires adéquats afin que ces derniers puissent leur apporter une solution. Mais il serait tout même, plus intéressant

[177]Gasperd Ferry, Nicalos Grorod et Simon Leguil, L'assurance des risques cyber: comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive, 2017, p69
[178]*ibid, p69*
[179]voir la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance.

d'impliquer les assureurs dans ce projet, car ils les premiers acteurs à accompagner les entreprises dans leur cyber-résilience.

En plus les Etats doivent démontrer plus d'initiative, ou favoriser l'initiative sur le processus de cyber résilience, et notamment en matière de formation et de prévention du risque[180]. C'est ce qu'avait compris Paul Ash[181], en 2012, en créant le *National Cyber Policy Office* (NCPO) afin de coordonner et diriger l'élaboration et la mise en œuvre de la politique de la cybersécurité de la Nouvelle-Zélande. Le NCPO mène également des activités de sensibilisation avec le secteur privé sur la politique de la cybersécurité. Il promeut la coopération entre les différents acteurs concernés, dont les assureurs font partie, et avise le gouvernement Néozélandais en matière de cybersécurité[182].

La mise en place d'une plateforme peut être une solution de facilitation des échanges entre acteurs, mais certains vont plus loin en demandant la garantie de l'Etat en dernier ressors. Cela se comprend car, même si le scénario ne s'est pas encore réalisé, une attaque cyber qui paralyserait tout un secteur qui représente 90% du commerce mondial, serait difficile à gérer par l'industrie de l'assurance, en raison des montants en jeu. Sachant qu'assureurs comme réassureurs son de surcroît directement exposés au pareil lui-même[183]. D'ailleurs dans un rapport publié en 2017 par Allianz Global Corporate& Specialty intitulé « Global Claims Review: Liability in Focus », on apprend que « *des sinistres dépassant 1 milliard USD vont, en effet, devenir de plus en plus communs, et ne concerneront plus uniquement les seuls Etats-Unis et l'Europe*[184] ». Evidemment le risque cybernétique fait partie des risque émergent qui peuvent être fréquents dans cette décennie. Et le secteur étant presque le dernier secteur à s'y investir peut être la nouvelle cible des attaquants en raison de son manque de connaissance pour ce risque.

[180] Roxanne DESLANDES, « Présentation des programmes de cyberassurance et de leurs limites », Mémoire, 2017, p40
[181] Représentant spécial du Premier ministre sur le cyberespace et le numérique, coordonnateur du cyberespace au Département du Premier ministre et du Cabinet, Nouvelle-Zélande.
[182] Roxanne DESLANDES, « Présentation des programmes de cyberassurance et de leurs limites », Mémoire, 2017, p40
[183] L'assurance Cyber: un risque catastrophe ou un placement d'avenir?, PwC, https://www.pwc.fr/fr/decryptages/securite/lassurance-cyber-un-risque-catastrophe-ou-un-placement-davenir.html
[184] « Global CliamsReview: Liability in Focus », Allianz global Corporate& Specialty, Report, 2017, p5.

B) L'Etat, garant en dernier ressort

Dans la première partie nous avons démontré la nature systémique du risque cyber, qui peut atteindre des proportions inimaginables en cas d'incident majeur. C'est un risque comparable au risque pandémique dans certains cas. En effet, les assureurs sont très frileux pour la prise en charge du risque pandémique. Ils considèrent que la pandémie constitue un risque atypique, voire « inassurable » pour les assureurs : de très grand ampleur, elle touche tout le monde, partout et en même temps. Et en parlant de crise la FFA a estimé que : « *les pertes d'exploitation des entreprises françaises couvertes par une garantie en pertes d'exploitation se sont montées à 60 milliards d'euros durant le confinement, soit environ l'équivalent de 100 ans de collecte primes*[185] ». « *Ces pertes ne peuvent être supportées par aucun acteur à part l'Etat*[186] » souligne la présidente de la Fédération Française de l'Assurance. Il est donc essentiel que des acteurs externes au marché comme l'Etat interviennent pour sécuriser et rassurer les assureurs.

Dans le secteur maritime l'intervention de l'Etat comme garant en dernier ressort est d'une importance capitale. C'est l'un des secteurs où les cyber attaques vont probablement augmenter, en raison de sa transformation numérique accélérée, mais aussi de son déficit de connaissance du risque cyber. Avec la nature systémique du risque cyber, ces attaques peuvent s'avérer catastrophique pour le secteur maritime. En effet, avec pertes probables à coût de milliard de dollars, l'aide de l'Etat peut être fondamental, comme c'est la cas pour les actes terroristes, pour lesquels l'Etat intervient via la Caisse Centrale de Réassurance (CCR). La CCR offre une couverture illimitées des risques exceptionnels, non assurables en France, qui naissent de l'utilisation de transport de toute nature ou se rapportent à des biens en cours de transport[187].

Pourtant certaines voix s'élèvent pour réfuter, la pertinence de l'Etat garant vis-à-vis des risques cyber. Dans leur mémoire intitulé l'*assurance des risques cyber: comment*

[185] Benoit Toussaint, Carole Guirado, AFP, « Une assurance contre le Covid-19 et les menaces futures? Les 5 points clés du problèmes, La Tribune, 01 juin 2020.
[186] Voir la tribune de Florence Lustman, Présidente de la FFA, en date du 02 avril 2020, https://www.ffa-assurance.fr/actualites/mais-que-font-les-assureurs-dans-cette-crise-tribune-de-florence-lustman {Consulté le 6 aout 2020}.
[187] « L'assurance maritime: évolution de la perception du risque », ISEMAR, Note de synthèse N° 192, Septembre 2017.

tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive?, le groupe de chercheurs, après avoir démontrer les situations dans lesquels l'Etat peut être garant (dans l'assurance obligatoire avec le fonds de garantie des assurances obligatoires de dommages (FGAO) ou dans les catastrophes naturelles ou actes terroristes), souligne que « *si des actes de terrorisme utilisant des méthodes numériques venaient à engendrer des dommages corporels et matériels, les mécanismes en place interviendraient normalement*[188] ». Ce qui veut dire que si un acte de terrorisme s'organise avec des moyens technologiques, le fonds intervient. On se demande alors si une cyber attaque peut être qualifiée d'actes terroriste. Dans quels circonstances ou à l'aide de quels instrument peut-on qualifier une cyber attaque d'acte terroriste? En tout cas l'Office des Nations Unies contre la drogue et le crime souligne dans un rapport[189] publié en 2014 que « *les cyberattaques présentent parfois les caractéristiques d'un acte de terrorisme, notamment la volonté fondamentale de faire naître la peur à des fins politiques ou sociales* ». Pour eux, il est inconcevable que l'Etat intervienne en garantie d'un risque d'entreprise ou pire, d'un risque juridique.

Tout compte fait, il est important de se rappeler que le risque cyber peut atteindre des proportions insupportables pour les assureurs, dans les dix prochaines années, que seul l'Etat pourra assumer. Mais des solutions alternatives apparaissent de plus en plus pour se prémunir des risques cyber, même si leur efficacité reste à démonter.

Sous-section 2. L'externalisation de la protection des Systèmes informatiques: Prestations Cloud

L'externalisation de la protection des systèmes information est une solution exploitable mais comme tout processus il a des avantages (A) et des inconvénients (B).

A) Avantages

Selon une étude menée conjointement par Bessé et PwC, les solutions des prestataires Cloud représente en 2017 près de 50% des services informatiques apportés aux

[188] Gaspard Ferey, Nicolas Grorod, Simon Leguil, « L'assurance des risques cyber; comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive?, Telecom, Paris Tech, 2017, p68.

[189]« L'utilisation de l'internet à des fins terroristes », Office des Nations Unies contre la drogue et le crime, Rapport 2014, p12.

entreprises[190]. En effet certains compagnies maritimes optent pour le transfert de la sécurisation de leurs infrastructures informatiques à bord et à terre à des prestataires de clous. Le Cloud est une technologie qui permet de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels qui sont habituellement stockés sur l'ordinateur d'un utilisateur, voire sur des serveurs installés en réseau local au sein d'une entreprise[191]. Cet outil donne la possibilité aux compagnies maritime, qui ne sont pas en mesure d'assurer la gestion des risques, d'externaliser la protection de leur SI par des prestataires Cloud. A travers le Cloud, les prestataires peuvent améliorer le contrôle et la visibilité des nouveaux risques cyber tout au long de la chaîne de valeur maritime.

Depuis de nombreuses années, on constate une transformation numérique du secteur maritime. Cette transformation a certes, des avantages, mais expose les compagnies maritimes aux cybermenaces qui pourraient avoir de graves conséquences sur leur économie. C'est la raison pour laquelle des prestataires Cloud comme le groupe[192] ABS et Atos collaborent pour offrir une solution de sécurité des technologies de l'information (IT) et des technologies opérationnelles (OT).

Il est donc important pour les compagnies maritimes qui n'optent pas pour le transférer du risque cyber vers les assurances, de se retourner vers ces prestataires, pour une cybersécurité de bout en bout de leurs données. Et à ce titre réduire les risques cybernétiques dans la chaîne d'approvisionnement globale.

Dans le secteur maritime, les données constituent un actif très précieux, sur lequel l'activité de l'entreprise ainsi que son développement en dépendent fortement. C'est pourquoi, il faut, au-delà de l'aspect confidentiel et stratégique, tenir compte de la sécurité juridique des données, qui peuvent être considérées comme très sensibles[193]. C'est le cas par exemple de la gestion des mots de passe, dont la fréquence de son changement et son

[190] « Les dirigeants d'ETI face à la menace cyber », BESSÉ-PwC, Enquête, Mars 2018, p16.
[191] « Etude sur les « cyber risques » et leur (ré)assurabilité », APREF, juin 2016, p33
[192] https://atos.net/fr/2019/communiques-de-presse_2019_10_15/le-groupe-abs-et-atos-collaborent-pour-offrir-la-premiere-solution-de-securite-it-ot-a-destination-des-operations-maritimes-et-offshore-globales
[193] Op. cit. p34.

format ne sont pas adapté, ou de la gestion des droits d'accès à bord des navires, qui apparaît plus préoccupante et faiblement maîtrisée[194].

L'externalisation de la protection des SI à travers les prestataires Cloud, est certes, une solution pour compagnies maritimes, mais comme tout outil informatique, le Cloud est vulnérable et peut être soumis à des attaques cyber.

B) Inconvénients

Il n'est pas rare de voir des prestataires Cloud proposer leurs services à plusieurs entreprises, de différents secteurs d'activité. En effet, les entreprises, dans la volonté de renforcer la protection de leurs données, font appel à des prestataires Cloud. Le plus souvent, elles sont hébergées chez un même prestataire de services. De ce fait, cette concentration d'entreprises au sein d'un même hébergeur augmente le risque systémique de nature à les impacter considérablement, en cas de défaillance du prestataire.

L'externalisation des services informatiques des entreprises vers des prestataires de services Cloud permet une réduction des coûts d'infogérance ainsi qu'un gain en sécurité[195], mais cela implique dans certain cas, un manque de maîtrise du risque cyber, avec une visibilité amoindri du niveau de sécurité des systèmes informatiques et une capacité relative des entreprises, surtout les PME, à pouvoir vérifier l'adaptation des solutions à leurs propres enjeux. Cette question des prestataires informatiques préoccupe les assureurs car la plupart de leurs clients sont hébergés par des prestataires informatiques. On se demande ce qui se passerait si un prestataire informatique est touchée par un malware.

En février 2016, l'université de Cambridge en collaboration avec RMS, publie une étude[196] basée sur le scénario d'accumulation de test de résistance de plusieurs entreprises hébergées par le même prestataire de service Cloud (CSP). Ils démontrent que les pertes commerciales que peuvent subir les clients, en cas de défaillance technique du fournisseur,

[194] « Cyber sécurité, Evaluer et protéger le navire », ancien Ministère de l'environnement, de l'énergie et de la mer, Rapport, Edition septembre 2016.
[195] Op. cit. p34
[196] « Managing cyber insurance accumulation risk », Cambridge, center for riskstudies&Risk Management Solutions (RMS), Report, February 2016, p 40.

sont conséquents. Il s'agit, évidemment, d'une défaillance technique mais on peut l'envisager dans un scénario de cyberattaque, et les conséquences seront encore plus désastreuses, à cause de la nature systémique du risque. En effet, en cas d'indisponibilité des services du fournisseur, il est probable de constater un arrêt d'exploitation des entreprises hébergées. Et dans ce cas, quid des entreprises ayant souscrites une cyberassurance couvrant les pertes d'exploitation ?

Il existe plusieurs prestataires de services Cloud dans le monde, mais dans cette étude nous allons nous concentrer sur le plus important, Amazon Web Services (AWS). Dans son contrat dénommé « *Contrat Client AWS* », il utilise sa position dominante sur le marché, en imposant des clauses contractuelles, sans négociation possible de la part des entreprises clients. Il précise dans le préambule « *le présent contrat prend effet lorsque vous cliquez sur le bouton ou cochez la case « J'accepte » relatifs aux présents conditions générales…* ». Et plus loin dans le contrat, AWS, se déresponsabilise de toute suppression, destruction, dommages, perte ou défaut de stockage des données[197]

Peut-être la création de référentiels en matière de cybersécurité pourrait faciliter les choses. Mais serait-il réaliste, voire même légitime de parler de normes, de référence ou de contrôle? Quel référence construire dans la durée dans un domaine où les évolutions technologiques sont permanentes?

Sous-section 3. Des solutions envisageables

Au-delà des solutions que proposent l'industrie de l'assurance et des pistes de solutions qui peut émaner d'acteurs externes, les compagnies peuvent envisager de s'auto-assurer ou « *self financing* » (A), ou chercher les biens fait de la blockchain (B).

A) L'auto-assurance ou « self financing »

Il est possible que certaines entreprises, de par leur taille et la nature de leurs activités, s'exposent à des risques très élevés que les assureurs hésitent à couvrir. Avec

[197] Voir à titre d'exemple les clauses 10 et 11 du Contrat Client AWS, relatives à l'exonération et à la limitation de responsabilité - https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement-French_Translation_(2020-06-30)-new.pdf

près de 9 milliards de tonnes de marchandise transportées par an[198], la voie maritime représente près de 90% du commerce mondial. Au cours de la dernière décennie, on a constaté que ce secteur devient de plus en plus la cible d'attaques cyber, en raison certainement de la digitalisation. Mais comme, nous l'avons démontré précédemment, à l'heure actuelle, les acteurs ne disposent pas de toutes les pièces du puzzle pour la gestion du risque cyber. Si du côté des assureurs, les produits cyber sont en cours de maturité, les compagnies maritimes quant à elles, pensent que la solution est de renforcer leur niveau de sécurité. Il est vrai que les compagnies maritimes doivent, en ce qui concerne les risques technologiques, renforcer leur niveau de sécurité, mais cela ne suffit pas pour se prémunir du risque cyber.

Pour pouvoir faire face aux nouveaux risques majeurs, le secteur maritime, au-delà de cette maturité du niveau de sécurité, a besoin d'être accompagné par les assureurs dans la gestion du cyber risque.

Pourtant, certaines entreprises renoncent à payer des primes toujours plus élevées pour s'assurer, estimant que le capital pourrait être mieux investi[199]. Ils préfèrent se tourner vers l'auto-assurance ou « self-financing ». L'auto-assurance permet à une entreprise de ne pas souscrire un contrat d'assurance pour couvrir certains risques. Mais est-ce réalisable dans le cadre du risque cyber?

L'auto-assurance peut être une solution pour les compagnies maritimes de se protéger contre le cyber risque. En effet, elles peuvent investir sur leur niveau de sécurité et jouer sur l'aléa du risque. Mais force est de constater que le risque cyber est partout et peut se manifester sous diverses formes, allant d'un acte de malveillant qui visent des systèmes de communication et/ou de navigation[200], à une simple erreur humaine. Et nous savons que le facteur humain est le maillon faible en cybersécurité. Donc il ne peut y avoir de système infaillible, peu importe le niveau de maturité de la compagnie. A cet titre, l'auto-assurance peut certes, être une solution; mais les compagnies maritime se doivent de réfléchir en termes de transfert du risque vers l'assurance ; car concernant le risque cyber

[198] https://info.arte.tv/fr/le-commerce-maritime-mondial-infographies

[199] AndràsNovember et Valérie November, « Risque, assurance et irréversibilité », Revue européenne des sciences sociales - http://journals.openedition.org/ress/475 , {Consulté le 8 aout 2020}.

[200] « L'assurance maritime: évolution de la perception du risque », ISEMAR, Note de synthèse N°192, Septembre 2017.

un scénario catastrophe pourrait mettre en danger la pérennité de leur *business*, leur existence et entrainer leur faillite[201].

Éventuellement, les géants du monde maritimes peuvent se réunir et s'auto-assurer pour les risques cyber, comme c'est le cas pour la responsabilité civile des armateurs, avec les P&I Club. Cette auto-assurance peut se faire sous forme de pools ou de captives leur permettant de mutualiser ou de partager les grands risques entre membre du groupe. On admet tout de même, qu'il serait difficile de conceptualiser un tel club pour un risque potentiellement systémique, mais avec la collaboration des assureurs maritimes comme consultants en risque, le défi est relevable.

B) La blockchain: un outil efficace pour se prémunir du risque cyber?

De nombreux secteurs sont en train d'étudier les applications de la blockchain. Cette nouvelle technologie pour le stockage, la traçabilité et la transmission de données, séduit de plus en plus dans le secteur maritime. A la base la Blockchain, est « *une application informatique qui utilise des techniques cryptographiques permettant à des entités de réaliser entre elles des opérations sans l'intervention d'un tiers de confiance*[202]. » Le monde maritime a très vite adopté cette innovation, en raison de la charge administrative incroyablement colossale, qui incombent les acteurs. Cette application peut permettre de réduire considérablement le temps passé dans la collecte, la consolidation et la confirmation des données nécessaire à l'établissement de documents de transport.

La blockchain peut être un moyen, pour les armateurs de se protéger contre le risque cyber et plus précisent de protéger leurs données essentielles. En effet la particularité de la blockchain est que les données qui y sont, en principe, infalsifiables et indestructible, en raison de l'impossibilité de modifier le contenu de ces serveurs et ordinateurs sans consensus commun[203]. De ce fait, cette technologie peut être un outil très

[201] Philippe Cotelle, Philippe Wolf, Bénédicte Suzan, « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance », Rapport de recherche, IRT SystemX, 2016.
[202] Jean-Guillaume, Pascal Lafourcade, Ariane Tichit, Sébastien Varette, « les blockchains en 50 questions: Comment comprendre le fonctionnement et les enjeux de cette technologies innovante », Dunod, Septembre 2018.
[203] https://www.lantenne.com/La-Blockchain-s-invite-dans-le-maritime_a36760.html

adapté aux risques cyber. La plupart des assureurs maritimes reconnait, un problème d'intervention tardive lors d'une attaque cyber. Ils peinent non seulement à comprendre la nature et l'occurrence des sinistres, mais aussi à détecter rapidement les attaques cyber. C'est pourquoi, nous estimons que, la blockchain pourrait être une véritable révolution, dans la maîtrise du risque cyber, tant pour les compagnies maritimes, que pour les assureurs.

Dans le secteur maritime, plusieurs compagnies ont franchi le pas; à l'image de Maersk Line qui a mis en place, avec IBM, une plateforme blockchain de suivi d'expédition au niveau mondial. Au niveau des compagnies d'assurance, la blockchain, peut également être uns piste exploitables pour le développement du marché cyber. D′autant plus que 80% des risques dans le monde ne sont pas assurés, et restent à la charge des individus ou des gouvernements, « *la piste de la blockchain, au-delà d'une numérisation, va introduire l'arrivée du produit d'assurance en temps réel qui pourra enfin couvrir les risques les plus incertains et complexes*[204]. », souligne Shuan Crawford[205].

Toutefois, il faut noter que la technologie de la blockchain, repose sur la cryptographie à clé publique et des primitives telles que les signatures numériques et les fonctions de hachage, ce qui peut donner une fausse impression de sécurité. Dans l'analyse de sécurité de la blockchain, on néglige, souvent, que les protocoles cryptographiques ont leur limites et que la sécurité globale comprends non seulement la technologie, mais aussi les personnes et les processus[206].

Enfin précisons que la blockchain, n'est qu'une piste de solution pour les compagnies maritimes mais aussi pour les assureurs, car à l'heure actuelle, cette technologie n'est pas réglementée; ce qui entraîne des incertitudes juridiques et des zones grises.

[204] Morgan Remy, « La blockchain au service de l'assurance maritime », https://www.argusdelassurance.com/tech/la-blockchain-au-service-de-l-assurance-maritime.136654 {Consulté le 11 août 2020}.
[205]global Vice Chair of Industry chez EY.
[206]https://www2.deloitte.com/ch/fr/pages/risk/articles/blockchain-security.html

CONCLUSION :

L'avenir du marché cyber n'est certes pas tout tracé, mais les signaux sont assez positifs pour nous laisser dire qu'il a un avenir prometteur. Le potentiel du marché fait qu'assureurs et réassureurs s'intéressent à ce marché. Avec un risque qui peut coûter entre 100 et 500 milliard par an aux entreprises, il est de l'intérêt de tous les acteurs de secteur maritime de se prémunir contre ce risque. La plupart du temps, les compagnies maritimes ne connaissant pas grand-chose au risque cyber, optent pour son transfert au marché de l'assurance.

Ce transfert, au regard de la fréquence de attaques cyber deviendra de plus en plus viable. Même si l'enjeu est plutôt de transférer ce risque au marché financier pour disposer de plus de capacité. Il est évident que l'assurance du risque cyber peut paraitre problématique, mais pas impossible. Donc il est du ressort de l'industrie de l'assurance de trouver des solutions pouvant aider les compagnies dans leur politique de cyber-résilience. Et comme le disait Mme Pouclet Juliane dans son mémoire intitulé *« les navires autonomes: vers le renouvellement du facteur humain et l'avènement de nouveaux risques » : « les hommes à terre, les compagnies, les inspecteurs, assureurs, concepteurs, des systèmes vont devoir acquérir de nouvelles compétences , se plier à de nouvelles réglementations, ou participer à leur création, et surtout verront leur attributions changer à la fois pour faire face aux nouveaux risques et à leurs nouvelles responsabilités ».* Elle veut dire par là que le travail vient de commencer et qu'il faut que les acteurs du secteur maritime s'adaptent à la transformation du secteur qui engendrera sans doute l'avènement de nouveaux risques tels que le risque cyber.

Des nombreux assureurs cherchent à innover dans leurs produits assurantiels, en y intégrant la couverture du risque cyber, soit en complément soit façon autonome. Mais on ne doit pas se limiter seulement à proposer des solutions assurantielles parfois de manière partielle; il faut une coopération entre assureurs et assurés pour étude approfondie du risque dans le but de prévoir toutes les éventualités. Et comme nous l'avons étudié dans ce mémoire, le risque cyber fait par partie des dix (10) risques émergents de cette décennie.

Pour cette raison, il sera inconcevable de laisser les assureurs seuls absorber les conséquences d'un risque, dont les conséquences sont parfois inestimables. Les pouvoirs publics ont un rôle crucial à jouer dans cette lutte. Au-delà de l'apport des Etats, les compagnies peuvent s'auto-assurer pour le risque cyber, compte tenu des montants que peut engendrer une attaque cyber. Ainsi la création d'un pool ou club ne peut-elle pas résoudre le problème de capacité dans l'assurance du risque cyber?

A l'heure actuelle, le risque cyber est encore mal connu dans le secteur maritime. Les assureurs ne disposent pas de toutes les informations nécessaires leur permettant de quantifier le risque, en raison de sa complexité. Mais une chose est sûre c'est que le marché de l'assurance cyber est un marché en devenir et sera potentiellement la pierre angulaire des offres d'assurance. Mais avant d'en arriver là il va falloir que les acteurs de l'industrie maritime coopèrent pour adopter une stratégie proactive afin de préparer la cyber-résilience des compagnies maritimes face à un risque aussi particulier et évolutif.

ANNEXES

Annexe 1

Le classement des différents risques émergents et leur score en terme de probabilité d'occurrence et d'impact sur 1 et 5 ans.

CARTOGRAPHIE 2020 DES RISQUES ÉMEI
POUR LA PROFESSION DE L'ASSU
ET DE LA RÉASSU

Classement des risques*

	1 AN			5 ANS		
RANG		RISQUES	SCORE		RISQUES	SCORE
1	(0)	Cyber-attaques	(3,8 ; 3,5)	(0)	Cyber-attaques	(4,3 ; 4,1)
2	(+1)	Crise du système financier	(3,1 ; 3,8)	(+1)	Crise du système financier	(3,8 ; 4,0)
3	(+4)	Environnement économique dégradé	(3,3 ; 3,3)	(-1)	Dérèglement climatique	(3,5 ; 3,7)
4	(+6)	Risque de terrorisme	(3,1 ; 2,5)	(+4)	Environnement économique dégradé	(3,5 ; 3,5)
5	(+3)	Qualité des données et leur utilisation	(2,8 ; 2,8)	(+5)	Qualité des données et leur utilisation	(3,4 ; 3,4)
6	(+10)	Augmentation des sanctions règlementaires et du risque de non-conformité	(2,8 ; 2,6)	(+4)	Inadaptation aux nouvelles technologies	(3,2 ; 3,4)
7	(+5)	Poids règlementaire	(2,7 ; 2,6)	(+7)	Augmentation des sanctions règlementaires et du risque de non-conformité	(3,3 ; 3,1)
8	(0)	Risque politique global	(2,9 ; 2,3)	(+7)	Risque de terrorisme	(3,5 ; 2,8)
9	(-4)	Dérèglement climatique	(2,4 ; 2,8)	(+3)	Risque politique global	(3,4 ; 2,8)
10	(-8)	Croissance des inégalités et tensions sociales	(2,8 ; 2,2)	(-6)	Changement de normes comptables et du référentiel prudentiel	(3,1 ; 3,1)
11	(-7)	Changement de normes comptables et du référentiel prudentiel	(2,5 ; 2,4)	(-2)	Croissance des inégalités et tensions sociales	(3,4 ; 2,8)
12	(-1)	Inadaptation aux nouvelles technologies	(2,3 ; 2,4)	(+1)	Dégradation de l'environnement	(3,3 ; 2,8)
13	(-7)	Risque politique européen	(2,3 ; 2,3)	(-7)	Disruption du secteur de l'assurance	(2,9 ; 3,2)
14	(-1)	Impérialisme économique	(2,4 ; 2,0)	(-7)	Poids règlementaire	(3,1 ; 2,9)
15	(0)	Dégradation de l'environnement	(2,2 ; 2,0)	(+1)	Vieillissement de la population	(2,9 ; 3,0)
16	(+3)	Ubérisation de l'économie	(2,2 ; 1,9)	(-11)	Risque politique européen	(3,1 ; 2,8)
17	(+1)	Flux migratoires	(2,6 ; 1,4)	(+1)	Impérialisme économique	(3,0 ; 2,7)
18	(-2)	Judiciarisation et pression sociale	(2,1 ; 1,9)	(-1)	Ubérisation de l'économie	(2,9 ; 2,5)
19	(-5)	Disruption du secteur de l'assurance	(1,8 ; 2,1)	(+2)	Flux migratoires	(3,3 ; 2,1)
20	(+1)	Risque politique français	(1,8 ; 1,9)	(0)	Risque politique français	(2,8 ; 2,6)
21	(+1)	Dégradation de l'habitat	(1,7 ; 1,8)	(-1)	Judiciarisation et pression sociale	(2,7 ; 2,4)
22	(+1)	Vieillissement de la population	(1,6 ; 1,8)	(0)	Dégradation de l'habitat	(2,5 ; 2,3)
23	(-3)	Augmentation du risque épidémique	(1,4 ; 2,0)	(0)	Augmentation du risque épidémique	(2,1 ; 2,6)

Note de lecture : À 1 an, le risque de cyber-attaque est placé en première position, comme lors de l'édition 2019 de la cartographie. Le score (3,8 ; 3,5) en termes de probabilité d'occurrence et d'impact potentiel respectivement est le plus élevé. À 5 ans, ce risque occupe également la première place, comme en 2019, avec toutefois un score encore plus élevé (4,3 ; 4,1).
Note : Les scores de probabilité et d'impact sont additionnés pour déterminer le classement des risques.

* Source : Cartographie 2020 de la profession de l'assurance et de la réassurance.

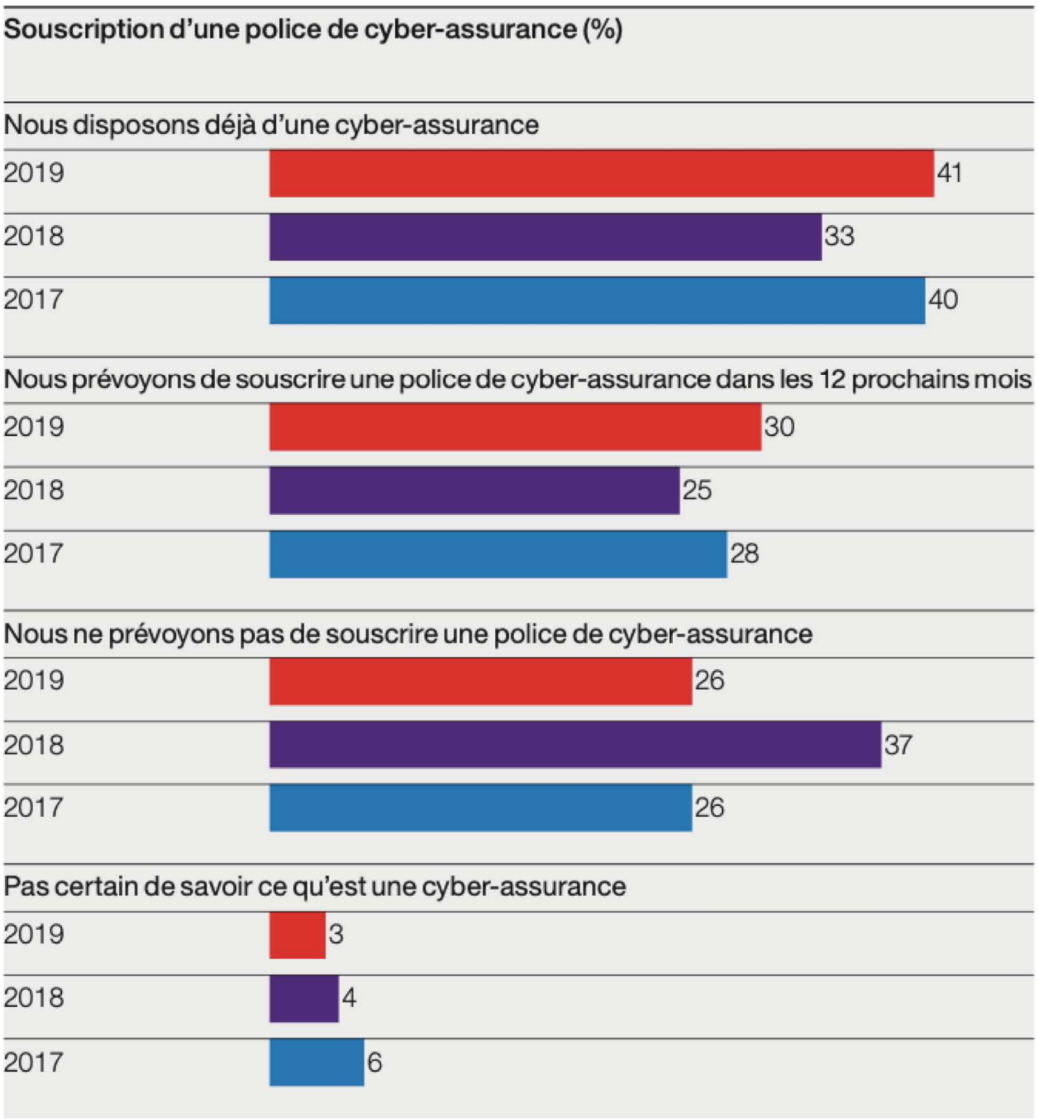
Annexe 2:

Analyse des primes pour les contrats cyber, dommages aux biens et responsabilité civile.

Source : UK Cyber security : The Role of Insurance in Managing and Mitigating the Risk – Marsh 2015

Annexe 3:

Dans ce tableau on peut observer que les souscriptions d'une polices d'assurance en 2019 varient entre 30 et 40% des entreprises, tous secteurs confondus. Et que dans les entreprises ayant déjà souscrites une police d'assurance cyber, plus de la moitié sont des grandes entreprises, contre 27% d'entreprise de moins de 50 salariés.



Source rapport Hiscox 2019 sur la gestion des cyber-risques

BIBLIOGRAPHIE:

I. THÈSES ET MEMOIRES :

Thèse :

- COSTE, B. « *Détection contextuelle de cyber attaques par la gestion de confiance à bord d'un navire* », Ordinateur et société, Ecole Nationale Supérieure Mines-Télécom Atlantique, 18 Décembre 2018, https://tel.archives-ouvertes.fr/tel-02079063 , 171 pages.

Mémoires :

- DESLANDES, R. « *Présentation des programmes de cyberassurance et de leurs limites* », Mémoire, 2017, 81p.
- FEREY, G; GROROD, N; LEGUIL, S. « *L'assurance des risques cyber, Comment tirer le meilleur parti de l'assurance dans un contexte de numérisation intensive?* », Mines Paris Tech, 2017.
- POUCLET, J. *« Les « navires autonomes » vers le renouvellement du facteur humain et l'avènement de nouveaux risques* », Université de Lille, 2019, 150p.

II. TEXTES OFFICIELS ET REGLEMENTATION

Loi :

- Code des assurances
- Code de la défense
- Code ISPS
- Code ISM

Réglementations

- Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous- secteur d'activités d'importance vitale « Transports maritime et fluvial » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense– JORF du 25 août 2016

- Décret n°2015_351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale
- Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
- Directive Network and Information Security (NIS) :
- https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Règlement (UE) 2016/679 du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), du 27 avril 2016. (RGPD).

OMI

- Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3 5 July 2017
- ISO/IEC 27001, Technologies de l'information, Techniques de sécurité, Systèmes de management de la sécurité de l'information, Exigences, 2013.
- Résolution MSC.428(98) « *Maritime Cyber Risk Management in Safety Management Systems* », 16 June 2017.

III. ENQUÊTES:

- BESSÉ-PwC, « *Les dirigeants d'ETI face à la menace cyber* », , Enquête, Mars 2018, p16.

- March, Benchmarking trends: *« Interest in cyber insurance continues to climb* », avril 2014.

- OPTIMIND, RGPD, *« Analyse d'impact des traitements sur les données personnelles - AIPD. Où en êtes-vous?* », 2019

- Ponemon Institute, « *2016 Cost of Cyber Crime Study & the Risk of Business Innovation* », Octobre 2016, 36p.

IV. ARTICLES ET REVUES:

- Armateur de France, « *La gestion des cyber-risques maritimes, Décryptage réglementaire* », Note de décryptage, Octobre 2019.
- Andràs November et Valérie November, *« Risque, assurance et irréversibilité* », Revue européenne des sciences sociales - http://journals.openedition.org/ress/475 , {Consulté le 8 aout 2020}.
- BAUMARD Philippe, *« La cybercriminalité comportementale : historique et régulation* », Vol 3, JO - Revue française de criminologie et de droit pénal (RFCDP)
- BESSE, Salon International Pacific Sydney, Communiqué de presse, Octobre 2019
- EDORH-KOMANE, P.A. « *Les menaces cyber dans le secteur maritime: a-t-on déjà envisagé tous les scénarios?* », 20 Avril 2020, 4p.
- HASSLER, A. *« Assurer, Réassurer et titriser les cyber-risques* », FFA, Revue risques, N° 120, Décembre 2019, p140.
- HEON, S et PARSOIRE, D. *« La couverture du cyber-risque* », extrait de la Revue d'Economie Financière, n° 126
- LASMOLES, O. « *Cybersécurité et navires sans équipages* », Lamy, DMF n°817, Octobre 2019
- LOOTGIETER, S *« Les risques cybernétiques dans le domaine des transports* », Lamy, DMF 775, décembre 2015
- MENDY, C. *« Emergence du besoin en cyber assurance* », Compte rendu du groupe de travail Cyber-risques, Institut des actuaires, 2017, p37.
- PAL, R. « *Cyber-Insurance for Cyber-Security. A Solution to the Information Asymmetry Problem »,* University of southern California, 2012
- PAL, R et GOLUBCHIK, L «*On Economic Perspectives of Internet Security: The Problem of Designing Optimal Cyber-Insurance Contracts*» University of Southern California, 2010.

- PAUQUET, W – BERCY, J – BENEDITTINI, M - CEIS, « *Cybersécurité dans le milieu maritime: défis et pistes de solutions* », Note stratégique, janvier 2017, p32.
- QUASHIE, F – ROLLAND, E – SPINEC, A – UBO, VALERO, C, ISEMAR.« *L'assurance maritime: évolution de la perception du risque* », Note de synthèse N° 192, Septembre 2017.
- ROMANOSKY, S. « *Examining the costs and causes of cyber incidents* », Journal of Cybersecurity, Vol.0, No.0, Août 2016, 15p.
- TOUSSAINT, B - GUIRADO, C - AFP, *« Une assurance contre le Covid-19 et les menaces futures? Les 5 points clés du problème* » , La Tribune, 01 juin 2020.
- VALERO, C – TOURRET, P. *« 20 ans d'apports des technologies aux industries maritimes »*, ISEMAR, note de synthèse, n°191, juin 2017.
- WISSEM AJILI, B.Y. « Les cyber risques: Nature, Etendue et moyens de couverture », Lamy, droit et Patrimoine, n°298, 1er janvier 2020.
- WILLIS TOWER WATSON. « *Willis Tower Watson launches innovate new cyber product for global airlines* », Press release, Avril 2017.

V. RAPPORTS:

- Allianz global Corporate & Specialty « *Global Cliams Review: Liability in Focus* », , Report, 2017, 40p.
- Ancien Ministère de l'environnement, de l'énergie et de la mer « *Cyber sécurité, Evaluer et protéger le navire* », Rapport, Edition septembre 2016, 37p.
- BANQUE DE FRANCE, « *Evaluation des risques du système financier français* », décembre 2019.
- CLUB DES JURISTES, *« Assurer le risque Cyber* », Janvier 2018
- CNUCED, *« Etude sur les transports maritimes* », 2018, 112p.
- *« Comment « débloquer » le marché de l'assurance cyber en France?* », Telecom Paris Tech, Alumni, Livre Blanc, Juin 2017, 22p.
- COTELLE, P – WOLF, P – SUZAN, B. *« La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance* », Rapport de recherche, IRT SystemX, 2016.

- CRO Forum « *Cyber resilience: The cyber risk challenge and the role of assurance* », Décembre 2014, 44p.
- H. KUNREUTHER, E. MICHEL-KERJAN, « *Insurability of (mega) terrorism risk : challenges and perspectives in OECD*» (2004)
- IFACI *« Cyber-risques: Enjeux, approches et gouvernance* », Juin 2018, 20p.
- IMO, « *Strategic plan for the Organization for the six-year period 2018 to 2023* ». A.1110(30), London. 8 December 2017.
- INTERPOL, « *Cybercrime : Covid-19 impact* », Août 2020.
- LEPETIT, Jean-François, « *Rapport sur le risque systémique* », Ministère de l'Economie, de l'industrie et de l'emploi, avril 2010
- Marsh Report : «*Continental European Cyber Risk Survey* », Octobre 2016, 16p.
- Office des Nations Unies contre la drogue et le crime « *L'utilisation de l'internet à des fins terroristes* », Rapport 2014, 179p.
- PwC, *« Insurance 2020 & beyond, Reaping the dividends of cyber resilience»*, 2015, p. 10.
- PwC, « *Le marché de la cyber-assurance: la révolution commence maintenant »*, janvier 20
- *Rapport Hiscox sur la gestion des cyber-risques*, 2019.
- SWISS RE, « *Cyber: Comment venir à bout d'un risque complexe?* », Sigma n°1, 2017, 40p
- Willis Towers Watson, *« Les marchés de l'assurance en 2020* », Note de conjoncture, septembre 2019.

VI. GUIDES:

- BIMCO and International Chamber of Shipping, « Cyber Security Workbook for on Board Ship Use », Ed. 2019. 158p.
- BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI : « *The Guidelines on cybersecurity on board ships, version 2.0, 2017* ».
- DGITM-Direction des affaires maritime « *Cyber Sécurité, évaluer et protéger le navire »*, Edition septembre 2016, 37 pages.

- DGITM-Direction des Affaires Maritimes « *Cyber Sécurité, renforcer la protection des systèmes industriels du navire »*, Edition janvier 2017, p3.

VII. SITES INTERNET :

- C. Biener, M. Eling et J. H. Wirfs, *«Insurability of cyber risk: an empirical analysis*» University of St. Gallen, janvier 2015. 32p, https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.html {Consulté le 4 juin 2020}
- https://www.lemonde.fr/europe/article/2007/06/27/l-estonie-tire-les-lecons-des-cyberattaques-massives-lancees-contre-elle-pendant-la-crise-avec-la-russie_928568_3214.html, {Consulté le 5 juin 2020}
- Nicolas Kampantais, « *Cyber Risks and Insurance in the marine Industry*», http://www.jdsupra.com/legalnews/cyber-risks-and-insurance-in-the-marine-32124/ {consulté le 8 juin 2020}
- https://www.marinelink.com/news/autonomous-shipping-cyber-hazards-ahead-471587 {consulté le 9 juin 2020.}
- https://www.atlas-mag.net/article/le-marche-de-la-cyberassurance-en-2019 {consulté le 12 juin 2020}
- https://www.ssi.gouv.fr/liste-produits-et-services-qualifies {consulté le 16 juin 2020}
- http://www.armateursdefrance.org/sites/default/files/decryptages/note_decryptage_-_gestion_des_cyber-risques_maritimes_21_10_19_vf.pdf {consulté le 16 juin 2020}
- https://www.ecologique-solidaire.gouv.fr/surete-maritime {consulté le 16 juin 2020}.
- https://www.optimind.com/fr/newsroom/enquetes/2019/09/19/rgpd-analyse-d-impacts-des-traitements-sur-les-donnees-personnelles-aipd/ {consulté le 18 juin 2020}.
- http://cyberguerre.numerama.com.via.snip.ly/obt3e4#https://cyberguerre.numerama.com/5194-easyjet-2-200-cartes-de-credit-divulguees-et-9-millions-de-clients-touches-dans-une-cyberattaque.html {consulté le 19 juin 2020}.
- https://www.legifrance.gouv.fr/affichTexte.do?categorieLien=id&cidTexte=JORFTEXT000039666574&dateTexte= {consulté le 19 juillet 2020}.

- https://www.willistowerswatson.com/en-BE/news/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch. {Consulté le 13 juillet 2020}.
- https://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/ {Consulté le 21 juillet 2020}.
- https://www.lesechos.fr/monde/europe/cyber-risques-le-lloyds-de-londres-veut-mettre-de-lordre-dans-les-contrats-1132705 {Consulté le 23 juillet 2020}.
- https://www.fmglobal.fr/products-and-services/products/cyber-resilience-solutions {Consulté le 27 juillet 2020}.
- https://www.cyber-cover.fr/uploads/assurance/garanties/5c59c5f9dbd91564441249.pdf {Consulté le 28 juillet 2020}.
- https://cybex-assistance.com/
- « Cyberassurance: digérer la part de risque, 20 septembre 2018. https://www.institutdesactuaires.com/magazine/article/cyberassurance-digerer-la-part-de-risques/2549 {Consulté le 30 juillet 2020}.
- « Réassurance: Et si le risque cyber bénéficiait d'un « filet de sécurité » de l'Etat?, Mariona Vivar, 2 mars 2017. https://www.newsassurancespro.com/reassurance-certains-risques-cyber-beneficiaient-de-garantie-detat/0169314696 {Consulté le 30 juillet 2020}.
- Aurélie Abadie, « Cyber réassurance, mode d'emploi », https://www.argusdelassurance.com/les-assureurs/cyber-reassurance-mode-d-emploi.151870 . {Consulté le 3 aout 2020}.
- Marie Caroline Carrière « Les entreprises françaises fortement investies par la cyber sécurité », https://www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/les-entreprises-francaises-fortement-investies-par-la-cyber-securite.168449 {Consulté le 4 aout 2020}.
- https://www.atlas-mag.net/article/lassurance-des-cyber-risques {Consulté le 5 aout 2020}.

- Brice Ducoum, « Industrie maritime et risque cyber », https://observatoire-fic.com/industrie-maritime-et-risque-cyber-par-brice-ducoum-groupe-eyssautier/ {Consulté le 5 aout 2020}.
- L'assurance Cyber: un risque catastrophe ou un placement d'avenir?, PwC, https://www.pwc.fr/fr/decryptages/securite/lassurance-cyber-un-risque-catastrophe-ou-un-placement-davenir.html {Consulté le 6 août 2020}
- https://atos.net/fr/2019/communiques-de-presse_2019_10_15/le-groupe-abs-et-atos-collaborent-pour-offrir-la-premiere-solution-de-securite-it-ot-a-destination-des-operations-maritimes-et-offshore-globales { Consulté le 6 août 2020}
- Virginie Bensoussan-Brulé, « Cyberattaques: l'assurance cyber risques », 22 mai 2017, https://www.alain-bensoussan.com/avocats/cyberattaques-assurance-cyber-risques/2015/03/11/ {Consulté le 6 août 2020}

TABLES DES MATIERES :