Mémoire de recherche

Master mention Droit de la mer et risque maritime parcours Droit International et Européen

Faculté des sciences juridiques, politiques et sociales | Université de Lille

Année universitaire 2022-2023

L'assurabilité du risque cyber en transport maritime

Autrice : KAMMOUN Yassamine

Directeur du mémoire :
VAN CAUWENBERGHE Patrick

Membre du jury de soutenance :
DUPONT Bénédicte

REMERCIEMENTS

Tout d'abord, je tiens à remercier chaleureusement mon directeur de mémoire, Monsieur Patrick VAN CAUWENBERGHE, pour sa disponibilité et ses précieux conseils qui m'ont été essentiels dans l'élaboration de ce travail. Assister à ses cours tout au long de l'année était un véritable plaisir et une révélation de ma passion pour le droit des assurances maritimes, qui me guidera, certainement, dans mes projets futurs.

J'exprime également mes remerciements les plus sincères à Madame Bénédicte DUPONT pour son honorable participation à ce jury, son enseignement et ses encouragements tout au long de l'année.

Ma gratitude s'étend également à tous les professeurs de ce Master, qui nous ont partagé leur savoir et ont renforcé notre passion pour le Droit Maritime.

J'adresse mes remerciements chaleureux à ma famille, qui bien que distante géographiquement, demeure proche de mon cœur. En particulier, à ma chère maman, merci pour ton soutien indéfectible et ton amour infini, qui ont été mes guides infaillibles tout au long de cette aventure académique.

A mes chers amis, ma deuxième famille en France, merci pour votre soutien inestimable et vos encouragements continus. Vous êtes la source d'inspiration qui illumine mes journées.

Enfin, je suis profondément reconnaissante à tous ceux que je n'ai peut-être pas mentionnés individuellement mais qui ont joué un rôle dans ce mémoire.

Ce travail de recherche est dédié à vous tous. J'espère qu'il vous rendra fiers.

Yassamine KAMMOUN

SOMMAIRE

SIGLES ET ABRÉVIATIONS

AIS : Automatic Identification System

AISC /IACS : Association Internationale des Sociétés de Classification

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

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

BIMCO : The Baltic and International Maritime Council

BMI : Bureau Maritime International

CC Re : Caisse Centrale de Réassurance

CESAM : Comité d'Etudes et de Services des Assureurs Maritimes

CESIN : Club des Experts de la Sécurité de l'Information et du Numérique

CMI : Comité Maritime International

CMS : Content Management System

CNIL : Commission Nationale de l'Informatique et des Libertés

CyRiM : Cyber Risk Management Project

DMF (Revue) : Droit Maritime Français

DGPS : Differential Global Positioning System

DPO : Data Protection Officer

ECCC : The European Cybersecurity Competence Centre

ECDIS : Electronic Chart Display and Information System

ENISA : The European Union Agency for Cybersecurity

FGAO : Fonds de Garantie des Assurances Obligatoires

GPS : Global Positioning System

IA : Intelligence Artificielle

ISM (code) : International Safety Management

ISPS (code) : International Ship and Port Facility Security

IUMI : International Union of Marine Insurance

LPM : Loi de Programmation Militaire

MSC : Maritime Security Council

NIS (Directive) : Network Information Systems

NTIC : Nouvelles Technologies d'Information et de Communication

OCDE : Organisation de Coopération et de Développement Économiques

OIV : Opérateurs d'Importance Vitale

OMI : Organisation Maritime Internationale

OTAN/NATO : Organisation du Traité de l'Atlantique Nord

OSE : Opérateurs de Services Essentiels

P&I Club : Protection and Indemnity Club

RGPD : Règlement Général sur la Protection des Données

SGDSN : Secrétariat Général de la Défense et de la Sécurité Nationale

SGS : Système de Gestion de Sécurité

SI : Système Informatique

SIIV : Systèmes d'Information d'Importance Vitale

SOLAS : The International Convention for the Safety of Life at Sea

UE : Union Européenne

VTS : Vessel Traffic Services

INTRODUCTION GÉNÉRALE

De nos jours, l'espace numérique, tout comme l'espace maritime, constitue *"la matrice des échanges internationaux contemporains"*[1], qu'il s'agisse d'échanges commerciaux, financiers ou d'informations.

Au même titre que les océans ont offert historiquement des voies d'échange pour le commerce mondial, le cyberespace facilite, aujourd'hui, les communications entre individus et industries, à travers le globe.

A présent, à une époque où l'automatisation prend une place de plus en plus grandissante dans le commerce international, le secteur maritime, constituant une large proportion (environ 90 %)[2] du volume du commerce mondial, s'inscrit dans cette même dynamique. Ce nouveau milieu numérique *"infini,* (et) *propice à l'anonymat"*[3]*,* se voit interagir naturellement avec le milieu maritime.

"Jamais la mixité cyber et maritime n'a été aussi vraie d'un point de vue économique"[4]. Des navires autonomes aux ports intelligents, tout en passant par les systèmes de gestion de la chaîne d'approvisionnement, l'industrie maritime s'intègre, progressivement, dans une course effrénée vers la numérisation, afin de réduire les coûts et répondre aux exigences actuelles de la mondialisation.

L'océan devient, ainsi, un véritable espace *"connecté"*, qui continuera à se développer, tout en entraînant son lot de défis[5]. Tel que Nikolas Kamputais[6] l'a précisé, certes, *"la technologie a permis au secteur maritime d'améliorer sa production, ses coûts ainsi que la réduction du temps d'acheminement.*

---

[1] COUSTILLERE A.,*"Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ?"*, RDNA, n°789, 2016/4, p.44.
[2] KERMARREC Y., *" Cybersécurité et monde maritime : contexte, enjeux, challenges et opportunités",* DMF, nº 842, 1er janvier 2022, p.2.
[3] BENDER B., *"Un secteur uni pour faire face au risque cyber", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.29.
[4] FRONCZAK S., *"Lutte contre la cybercriminalité maritime : Prévôts de la mer contre pirates", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.45.
[5] MOREL C., "*L'océan : un espace numérique convoité ? Des mers de câbles"*, *éd.,* Institut Français des relations internationales, RAMSES, 2019, p.47.
[6] LASMOLES O., *"Cybersécurité et navires sans équipage"*, DMF, n°817, octobre 2019, p.779.

Néanmoins, les changements technologiques ont ouvert la porte à de nouvelles menaces et vulnérabilités…"[7].

Au sillage de l'intégration des nouvelles technologies informatiques dans le domaine maritime, et à mesure que les méthodes et les pratiques évoluaient, les risques qui y sont inhérents ont démontré leur aptitude à s'adapter à ces changements. La piraterie saurait illustrer parfaitement cette toile de fond.

En effet, dans un paysage maritime contemporain, les eaux jadis infestées de flibustiers révèlent une nouvelle forme de piraterie, plus discrète, mais non moins préoccupante, naviguant à travers les circuits numériques, plutôt que les horizons maritimes lointains.

"Les cybercriminels sont donc les dignes héritiers d'une tradition maritime ayant aujourd'hui pour espace de navigation, l'Internet (et) *les réseaux"*[8].

Par ailleurs, le fait de s'interroger sur les effets que les menaces cyber pourraient avoir sur l'espace maritime revêt d'un intérêt tout particulier.

Force serait donc de constater que le rapide développement de l'informatique et de l'automatisation dans le secteur maritime a entraîné une recrudescence des risques et des attaques cybernétiques. Dans cette optique, il paraît essentiel d'abord de délimiter ces notions afin de pouvoir recenser l'évolution du risque cyber dans le milieu maritime.

Plusieurs définitions ont été données de cette notion, mais aucune n'a fait l'unanimité entre les Etats et les différents acteurs de l'industrie maritime.

A titre d'exemple, l'Organisation Maritime Internationale (OMI) considère le risque cyber comme *"une situation dans laquelle, du fait d'informations ou de systèmes corrompus, perdus ou compromis, un actif*

---

[7] GIBBS J.-L., "*Cyber Risks and Insurance in the marine Industry"*, *in.*, Insurance Law360, March 14th, 2016, https://www.zellelaw.com/assets/htmldocuments/Cyber%20Risks_and_Insurance_in_the_Marine_Industry.pdf, Consulté le 20/08/2023, Version originale : *"Technology has permitted the maritime domain to improve production, cost and reduce delivery schedules. However, "these technological changes have opened the door to emerging threats and vulnerabilities as equipment has become accessible to outside entities"*.

[8] FRONCZAK S., *op.cit.,* p.45.

technologique est menacé par une circonstance ou un événement qui peut entraîner des défaillances opérationnelles, de sûreté ou de sécurité" [9].

De son côté, l'Organisation de Coopération et de Développement Économiques (OCDE), dans sa recommandation (VII.1) de 2015, définit cette menace telle qu'une *"catégorie de risques liée à l'utilisation, au développement et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit"*[10].

Enfin, certains assureurs appréhendent le risque cyber comme : *"tout risque de perte financière, d'interruption des activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologies de l'information"*[11].

Malgré les termes génériques de ces définitions, celles-ci semblent être limitées, étant donné qu'elles ne traitent pas du facteur humain, cause primaire des risques cyber[12].

Le risque de production d'une menace cybernétique aura pour conséquence le déroulement d'une cyberattaque. Cette dernière se présente comme l'ensemble "*des tentatives indésirables de voler, d'exposer, de modifier, de désactiver ou de détruire des informations via un accès non autorisé aux systèmes informatiques"*[13]. L'attaque cyber serait donc la manifestation d'une éventualité qu'est le risque cyber.

Pendant longtemps, dans le milieu du transport maritime, le risque cyber faisait partie d'un imaginaire, auquel on ne pensait jamais. Certes, l'intégration des technologies numériques dans l'habituel de ce mode de transport était rapide et bien accueillie. Toutefois, on ne s'est guère penché sur

---

[9] IMO Guidelines, note (12), *in.*, PIETTE G., Traité du Droit maritime, p.538.
[10] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.69.
[11] NORTHBRIDGE ASSURANCES, *"Qu'est-ce-qu'un cyber risque ?"*, https://www.nbins.com/fr/blog/ cyberrisques /qu-est-ce-qu-uncyberrisque, Consulté le 17 Août 2020, note (11), *in.,* THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, p.10-11.
[12] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, p.11.
[13] IBM, *"Qu'est ce qu'une cyberattaque ?",* https://www.ibm.com/fr-fr/topics/cyber-attack, Consulté le 26/08/2023.

les potentiels défis que ce nouveau mode de fonctionnement pourrait impliquer.

D'emblée, il convient de tracer les limites de l'opération du transport maritime. Selon l'article L5422-1 du code des transports, "*par un contrat de transport maritime, le chargeur s'engage à payer un fret déterminé et le transporteur à acheminer une marchandise déterminée, d'un port à un autre…*".

Avec l'inclusion des nouvelles technologies dans ce mode de transport, certaines tâches ont été déléguées à des machines automatiques et d'autres qui ne se faisaient, par le passé, que manuellement, sont devenues contrôlées à distance, par des ordinateurs…Bref, à l'heure actuelle, tout s'automatise dans le secteur du transport maritime. Conséquemment, la probabilité de production des cyber risques dans ce milieu s'accroît.

D'ailleurs, la majorité des études situent le coût global des pertes causées par la cybercriminalité, entre 100 et 500 milliards par an[14]. Ainsi, face à une telle gravité de dommages, se protéger contre les risques cyber s'avère, a priori, instinctif.

Cependant, il n'était pas du tout évident dans l'industrie du transport maritime de prendre en charge ces risques. La prise de conscience de la nécessité de se prémunir de la menace cyber était tardive dans ce milieu.

Nous pourrons expliquer ce retard par la complexité opérationnelle de ce mode de transport, qui implique plusieurs acteurs allant des armateurs aux opérateurs portuaires en passant par les gestionnaires de navires et les agents de fret. Cette chaîne logistique, assez complexe, peut rendre difficile la compréhension des risques cybernétiques et la mise en place de mesures de sécurité adaptées. En outre, la nouveauté de ce risque et le manque de précédents de cyberattaques, dans le secteur maritime, ont forcément contribué à ce sentiment de complaisance envers les menaces cyber.

Aujourd'hui, la situation est en train de changer. Les attaques récentes et la montée en puissance des cyber menaces ont amené une prise de

[14] HEON S., PARSOIRE D., *"La couverture du cyber-risque"*, Revue d'Economie Financière, n° 126, 2017/2, p.169.

conscience croissante au sein de l'industrie maritime. Les pertes et dommages causés par les cyberattaques, telles que la compromission des systèmes de navigation ou le blocage des infrastructures portuaires, ont mis en évidence la nécessité de renforcer la cybersécurité maritime et combler le retard.

Dans cette même logique, la couverture assurantielle de ces risques s'avère également importante. Afin de pouvoir analyser la position de l'industrie d'assurance quant à ce sujet, il est d'abord judicieux de rappeler que le contrat d'assurance est *"une convention par laquelle l'assureur s'engage à verser à l'assuré une somme d'argent réparant le préjudice subi en cas de survenance d'un sinistre, défini en échange du paiement d'une somme versée, soit à l'origine, soit périodiquement"*[15].

Autrement dit, l'assureur moyennant une rémunération (prime ou cotisation) s'engage à payer une prestation (indemnité, capital ou rente) à une autre partie (assuré ou bénéficiaire d'assurance), en cas de réalisation d'un risque déterminé. L'assurance sert alors à lutter contre un aléa, qu'on ne sait couvrir tout seul, si jamais il se produit.

En l'espèce, avec le terme *"assurabilité"* nous nous interrogeons sur la possibilité de couvrir le risque ou de l'exclure, donc la réponse du marché d'assurance face à l'émergence d'un risque. Dès lors, étudier la réaction de l'industrie assurantielle face au développement des risques cyber en transport maritime, présente de nombreux avantages tant pratiques que théoriques.

Pour commencer, traiter le risque cyber maritime est un sujet d'actualité, qui reste encore peu creusé. À chaque mention du mot *"Cyber"*, une série d'interrogations se déclenche, et tel qu'on a souligné dans un mémoire[16], apposer ce terme sur la couverture d'un quelconque ouvrage et les chances de son succès seront considérablement augmentées.

Ensuite, les différentes réglementations entourant les cyberattaques en milieu maritime sont toujours en évolution. Ce qui fait qu' analyser la manière

[15] Ministère de l'économie des finances et de la souveraineté industrielle et numérique, Fiches pratiques, *"Assurance"*, Direction générale de la concurrence, de la consommation et de la répression des fraudes, 04/08/2023, https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Assurance, Consulté le 27/08/2023.

[16] FEREY G., GROROD N., LEGUIL S., *"L'assurance des risques cyber"*, Sciences de l'Homme et Société, Mines Paristech, 2017, p.5.

par laquelle les polices d'assurance pourraient réagir à ces changements complexes, constitue un enjeu crucial pour l'industrie maritime.

En outre, d'un point de vue pratique, s'interroger sur la réponse assurantielle face au risque cyber maritime pourrait aider aux développement de nouveaux produits d'assurance. Il serait intéressant de voir la réaction du domaine de l'assurance qui s'adapte en permanence aux différents risques émergents.

Par ailleurs, se pencher sur la question d'assurabilité du risque cyber maritime, pourrait aider à l'anticipation de l'évolution de ces menaces et permettre de prévoir des solutions qui leur sont adaptées, afin de faciliter aux acteurs de l'industrie maritime l'évaluation, le contrôle et la protection contre la menace cybernétique.

Enfin, dans notre ère de plus en plus connectée, où les océans numériques se mêlent aux vastes étendues maritimes, le secteur du transport maritime se retrouve confronté à une réalité inédite. Les avancées technologiques ont apporté des avantages considérables en matière de navigation, de gestion des opérations portuaires et de suivi des cargaisons, mais elles ont également ouvert la voie à de nouveaux défis, notamment celui des cybermenaces. Les pirates modernes ne sont plus seulement ceux qui arpentent les vagues, mais aussi ceux qui naviguent dans les réseaux informatiques.

Face à cette menace, une question cruciale émerge :

Dans quelle mesure peut-on considérer le risque cyber en transport maritime comme un risque assurable ?

C'est précisément cette interrogation qui guidera notre mémoire, et nous aidera à délimiter d'abord l'étendue du risque cybernétique dans le secteur de transport maritime (chapitre 1), pour pouvoir par la suite examiner la réponse de l'industrie de l'assurance face au risque cyber maritime (chapitre 2).

CHAPITRE 1er - Controverse autour du cyber risque maritime

“ Le progrès, scientifique, technique, technologique, a toujours suscité des sentiments contrastés chez l'Être humain. La satisfaction, liée au gain de confort, de sécurité, de temps est contrebalancée par la crainte voire la méfiance, inspirées par des considérations éthiques, philosophiques, sociales ou politiques”[17].

Le monde maritime n’est pas épargné de ces préoccupations. En effet, avec l’hégémonie des nouvelles technologies informatiques et de communication (NTIC)[18] sur les méthodes et usages traditionnels de fonctionnement, les acteurs du milieu maritime s'avèrent particulièrement soucieux des risques que peut impliquer une dépendance accrue aux moyens digitaux. Partagés entre l’envie de gain de productivité et la méfiance des risques liés à l’usage des systèmes informatisés, ces acteurs cherchent à établir une sécurité non seulement économique mais aussi juridique, afin d’éviter des éventuelles pertes.

Dans les faits, le succès qu’ont eu les nouvelles technologies, en termes de gain de productivité et d’économie en transport maritime[19], a longtemps prévalu sur la sécurité maritime. Ce n’est que suite à la multiplication des cyberattaques contre les navires, les ports et les facultés maritimes que le besoin d'instaurer un cadre juridique pour prévenir ces risques et limiter leur impact s’est concrétisé.

Comme l’a souligné Laurent Banitz, *“...la sécurité est fille d’accidentologie”*[20]. Si aujourd’hui on devient de plus en plus conscients de la

[17] PIETTE G., *“La sécurité en droit maritime à l’épreuve des nouvelles technologies”*, *in.,* Transport et sécurité, LexisNexis, 2019, p.317.
[18] Définition NTIC selon le Dictionnaire du Droit privé, par BRAUDO S., Conseiller honoraire à la Cour d'appel de Versailles, *“L'acronyme NTIC (ou « TIC » équivalent de l'anglais ICT : « information and communication technologies ») désigne l'ensemble des technologies permettant de traiter des informations numériques et de les transmettre”.*
[19] PIETTE G., *“La sécurité en droit maritime à l’épreuve des nouvelles technologies”, op.cit.*, p.318.
[20] BANITZ L., *“Les cyber risques dans le monde maritime : de la prise de conscience aux actes”*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p. 23.

nécessité d'instaurer une culture de cybersécurité maritime, on le doit majoritairement aux leçons tirées des cyber attaques *"...dont les mers sont le théâtre..."*[21].

De nos jours, nous vivons dans un monde nouveau dont les contours sont modelés et sculptés, sous nos yeux, au rythme des nouvelles technologies numériques.

Cette digitalisation[22] croissante des activités maritimes demeure néanmoins une arme à double tranchant, provoquant une recrudescence de la sinistralité dans le secteur maritime (section 1). A ce niveau, bien qu'il semble judicieux de mettre en place un cadre légal et réglementaire adapté, la prise de conscience de l'importance d'une telle démarche n'a été que tardivement assimilée (section 2).

[21] BANITZ L., *op.cit.*

[22] Le terme digitalisation sera utilisé tout au long de notre analyse dans le sens de "numérisation"- c'est-à -dire- la traduction des données physiques en un format numérique et la transition vers les nouvelles technologies d'information.

Section 1 : Des risques cyber croissants face à la digitalisation du monde maritime

"...L'apport de la digitalisation se traduit depuis deux décennies par des changements sur les navires comme dans les ports, modifiant autant le management des outils, le travail des hommes, les processus logistiques et la commercialisation"[23].

Indubitablement, cette évolution technologique a offert des possibilités d'optimisation des opérations, de réduction des coûts et d'amélioration de l'efficacité dans le secteur maritime. Cependant, une dépendance accrue à ces outils numériques expose l'industrie maritime à de nouveaux risques (A), impliquant une hausse de la sinistralité et une multiformité des menaces cyber (B).

A)- Le développement d'une cyberdépendance des acteurs maritimes

Avec le développement exponentiel des moyens et technologies numériques dont nous sommes témoins ces dernières années, les entreprises du secteur maritime, suivant la tendance, tentent, de plus en plus, d'informatiser et d'automatiser leurs activités.

Cette évolution a même eu son néologisme dans le secteur maritime. On parle désormais de la *"marétique"* pour désigner *"l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations relatives aux activités maritimes, fluviales et portuaires"*[24].

Toutefois, de telles pratiques, si prises dans l'excès, augmenteraient considérablement la vulnérabilité des activités maritimes face aux menaces cyber. D'ailleurs, le secrétariat général de la Défense et de la Sécurité Nationale (SGDSN) a souligné cette idée dans son instruction relative à la sécurité maritime en affirmant qu' : *"au regard de la numérisation croissante*

[23] VALERO C., TOURRET P., *" 20 ans d'apports des technologies aux industries maritimes"*, Note de synthèse n°191, ISEMAR, Juin 2017, p.1.
[24] Livre bleu sur la marétique, Cluster Maritime Français, 2013, p.6.

des activités maritimes et portuaires, leur exposition aux menaces cyber est renforcée"[25].

Aujourd'hui, tant les navires en mer ou à quai que les infrastructures portuaires, tout est devenu une cible potentielle de cyberattaque. La mise en place de nombreux systèmes d'information (SI) et réseaux informatiques a favorisé clairement la multiplication des menaces cyber[26].

En effet, selon le baromètre des risques d'entreprises effectué par les assureurs, le risque cyber est placé pour l'année 2021, en troisième place après la pandémie[27].

Conséquemment, les acteurs du maritime s'inquiètent davantage sur l'avenir de leurs activités et les menaces susceptibles de toucher leur secteur.

Dans ce sens, une enquête publiée en 2022, par le secrétariat général de la mer en France, confirme ces propos. 64% des acteurs maritimes affirment que leur entité a déjà fait l'objet d'une tentative d'attaque cyber[28]. 36% de ces acteurs estiment que durant l'exécution de leur activité, ils font face à une exposition forte aux menaces cyber[29].

Cela nous amène à constater que l'automatisation du monde maritime est loin d'être sans effet. Certes, ce progrès technologique a facilité la transparence, la rapidité et le suivi. Mais, parallèlement, il a augmenté la vulnérabilité des navires et des ports[30].

En pratique, la cyberdépendance de l'industrie maritime peut être observée sur plusieurs niveaux.

Dans un premier temps, elle peut viser la construction de certains objets utilisés à bord des navires ou sur les ports.

---

[25] Secrétariat Général de la Défense et de la Sécurité Nationale, instruction interministérielle relative à l'organisation et à la coordination de la sûreté maritime et portuaire, 27 juin 2018, Instruction n° 230/ SGDSN/PSN/NP, p.13, https://www.sgdsn.gouv.fr/files/files/Publications/, Consulté le 15/08/2023.

[26] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *éd.,* 2022, p.545.

[27] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, DMF n°842, 01 janvier 2022, p.1.

[28] Voir annexe 1, p.111.

[29] *Ibid.*

[30] *Cf.,* THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, p.48.

Actuellement, avec le développement de la technologie d'impression 3D, de nombreux objets utilisés sur les navires ou pour effectuer des tâches sur les ports sont conçus par des imprimantes 3D. Cette technologie a reçu l'approbation de certaines sociétés de classification, notamment le "Bureau Veritas" qui a certifié une hélice imprimée en 3D, pour l'utilisation à bord d'un navire[31].

Dans le futur, il serait même envisageable que certains navires embarquent à bord, des imprimantes 3D, pour réparer plus rapidement en mer une pièce endommagée et la remplacer avec une pièce imprimée[32].

Cependant, étant un outil connecté, ces imprimantes demeurent susceptibles de faire l'objet de cyber attaques. Donc, on ne peut garantir le risque zéro, lors de la création. Dans cette hypothèse, suite à un défaut de conception, touchant un objet imprimé en 3D, utilisé dans un navire ou sur les ports, un accident pourrait survenir et causer des dommages. On serait, alors, face à une difficulté dans la détermination de l'origine du défaut et du responsable de la faute commise[33].

Dans un deuxième temps, la digitalisation peut concerner les systèmes de localisation des navires. A présent, le navire est devenu un objet traçable grâce aux technologies satellitaires[34], radars et GPS différentiel (DGPS)[35]. Avec l'*Automatic Identification System* (AIS)[36], on peut surveiller le trafic d'un navire, connaître son identité, sa position et sa route. En mettant en place des capteurs AIS sur les boués situées sur les côtes des passages étroits et sur les ports. On peut également établir un *Vessel Trafic Services* (VTS)[37], permettant,

---

[31] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, *op.cit.,* p.320.
[32] *Ibid.*
[33] *Ibid.*, p.325.
[34] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, *op.cit*.
[35] Selon la garde côtière canadienne, Le DGPS est une extension du système GPS qui utilise des radiophares terrestres pour transmettre les corrections de position aux récepteurs GPS. Il offre une méthode permettant de réduire la marge d'erreur de 30 mètres des positions calculées par les récepteurs GPS. Grâce aux récepteurs DGPS, il est possible d'obtenir une position exacte à 10 mètres près ou moins, publication Garde côtière canadienne, "*GPS et DGPS simplifiés"*, *éd.,* 2000, https://waves-vagues.dfo-mpo.gc.ca/, Consultée le 24/06/2023.
[36] *"L'AIS (Automatic Identification System), est un système d'échanges automatisés de messages entre navires. Il permet aux navires et aux systèmes de surveillance du trafic de connaître l'identité, la position et la route des navires"*, note (15), *in.*, PIETTE G., Traité du Droit maritime, 2023, *éd.*, Pedone, p.539.
[37] *"VTS (Vessel traffic services) ou les services de trafic maritime (STM) sont des systèmes à terre qui vont de la provision de simples messages contenant des renseignements aux navires - tels que la position d'autres trafics ou des avertissements de dangers météorologiques - à la gestion complète du trafic dans un port ou une voie*

à son tour, de programmer les escales des navires en liaison avec la capitainerie, les agents maritimes et les services portuaires[38].

En revanche, bien que *le tracing* du navire soit un apport majeur des technologies d'information, les risques de piratage et d'usurpation du signal et de ces données restent élevés. A titre d'exemple, un navire peut se trouver face à une situation de brouillage de signal. Dans ce cas, il ne serait plus en mesure de connaître sa position précise et sa navigation risque d'être erronée. Il pourrait, alors, se rendre sur des routes dangereuses où il fera face à des risques de piraterie maritime ou des récifs non découverts[39].

Notons que, selon Francis Baudu, arbitre maritime français, les navires peuvent faire l'objet principalement de deux types de menaces cyber. D'un côté, le brouillage *(jamming)* par lequel un navire *"...perd le fil de son information et répondra par une route erratique et une navigation erronée"*[40]. D'un autre côté, la mystification *(spoofing)* qui va faire signaler par l'AIS *"...des positions et indications de route erronées du navire, qui seront reçues et prises en compte par d'autres navires"*[41].

Dans ce même ordre d'idées, il est intéressant de noter que le traçage aujourd'hui ne se limite plus aux navires, mais peut aussi concerner ce qu'ils emportent à bord. D'ailleurs, tel qu'exposé par Eric Banel, directeur des affaires maritimes au sein du gouvernement français, lors du PARISMAT 2023[42], un projet de traçage de conteneurs en mer, œuvre de la société française Seatrackbox[43], serait présenté par la France à l'OMI, le 21 septembre 2023. Ce

---

navigable", OMI, https://www.imo.org/fr/OurWork/Safety/Pages/VesselTrafficServices.aspx, Consulté le 28/08/2023.

[38] VALERO C., TOURRET P., *" 20 ans d'apports des technologies aux industries maritimes"*, *op.cit.*, p.2.

[39] PIETTE G., Traité du Droit maritime, 2023, *éd.*, Pedone, p.540.

[40] BAUDU F.*, "Les cyber-menaces contre les navires et les installations portuaires",* Gazette n°43, CAMP, 2017, p.5.

[41] *Ibid.*

[42] Le rendez-vous ParisMat est un congrès annuel international du marché français de l'assurance maritime et de l'aviation, auquel de nombreux acteurs du secteur maritime peuvent participer, ainsi que les étudiants intéressés par ce domaine. Il est organisé par le CESAM (Comité d'études et de services des assureurs maritimes et transports). Les différentes interventions et tables rondes de la version de cette année (26-27 juin 2023), sont disponibles sur le site web de la conférence. https://www.cesam.org/ en/conference/lerendezvous /2023 /video.

[43] Seatrackbox est une start-up innovante, créée en 2017, qui propose le seul boîtier existant au monde, capable de tracer un container qui tombe à l'eau, n'importe où sur le globe. Ce système unique donne la localisation exacte des conteneurs en mer, en flottaison, à mi-eau ou coulés. Pour plus d'infos, consulter le site officiel : https://www.seatrackbox.com/.

projet a pour but de rendre obligatoire, partout dans le monde, la mise en place de capteurs sur les conteneurs, pour permettre de les localiser en cas de chute en mer. Solution ambitieuse, qui pourrait certainement éviter des problèmes financiers, des risques de pollution et des pertes considérables de marchandises et des conteneurs en mer. Par contre, aucune information n'a été présentée, lors du PARISMAT, sur la fiabilité et la résistance de ce système, face à une cyber attaque.

En somme, tel qu'il est illustré dans l'annexe 2[44], le navire moderne est, par définition, un objet connecté. Il se trouve, avec tout ce qu'il emporte à bord, au cœur *"...d'une bulle technologique mondiale..."*[45], qui le lie *"...à un écosystème complexe, celui d'une chaîne logistique mondiale interconnectée"*[46].

D'autre part, le développement technologique dans le milieu maritime a également impacté les infrastructures portuaires. Celles-ci se sont aussi engagées dans une course acharnée vers la modernisation, pour devenir ce qu'on appelle des *"smart ports"* ou *ports intelligents.* Par conséquent, leur exposition aux cyber menaces a augmenté, ce qui a été illustré à travers notamment l'attaque au port d'Anvers[47].

Concrètement, *un smart port* est un port qui se base principalement, dans son fonctionnement, sur l'interconnexion des systèmes d'information et de partage de bases de données, en vue de faciliter et fluidifier le contrôle douanier, les flux des navires, des passagers et du fret. Ces systèmes d'informations ont pour but de simplifier et d'accélérer les échanges entre les différents opérateurs de transport, les logisticiens, les chargeurs et les destinataires dans l'hinterland portuaire[48].

A ce titre, il est évident que dans le cas où ces échanges seraient perturbés, la cybersécurité portuaire serait compromise et l'infrastructure serait une cible d'attaque cybernétique.

---

[44] Annexe 2, p.111.
[45] MANET F.-C., *"La marétique, un enjeu essentiel pour l'humanité ?"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p. 80.
[46] *Ibid.*
[47] *Cf.,* Le Marin, *"Des terminaux pétroliers victimes d'une cyberattaque en Europe du nord",* publié le 03/02/2022, Consulté le 24/06/2023, https://lemarin.ouest-france.fr/secteurs-activites/shipping.
[48] PIETTE G., Traité du Droit maritime, *op.cit.*, p.540.

A ce propos, il est clair que la généralisation de l'informatique dans le secteur maritime ne s'est pas limitée aux navires, mais touche aussi les ports et la gestion des flux de cargaisons. Dans ce sens, plusieurs ports français, dont notamment le port de Rouen, utilisent, par exemple, le *Cargo Community System* (AP+) qui permet, grâce à une connexion internet, de contrôler et gérer de manière dématérialisée les flux de marchandises en import et export, les opérations de transbordement, les procédures administratives, commerciales et douanières, tout en assurant une traçabilité en temps réel de l'ensemble de la chaîne logistique[49]. Reste à savoir si réellement ces systèmes sont suffisamment sécurisés et fiables face à une cyber attaque.

L'automatisation dans le milieu maritime a atteint son apogée avec l'émergence des navires autonomes. Longtemps prônés pour leur sécurité face aux navires traditionnels et malgré les progrès remarquables réalisés en termes de réduction des accidents, ces navires demeurent manifestement menacés par le risque cyber. Gaël Piette remonte ceci à principalement deux raisons.

D'abord, un navire autonome est forcément plus équipé en systèmes informatiques qu'un navire traditionnel, d'où, un risque de cyberattaque plus élevé[50]. Ensuite, pour ce genre de navires, les délais pour traiter et connaître le problème informatique seront plus longs. Le navire serait, donc, plus fragile face à une potentielle cyberattaque[51].

A ce sujet, tel que relayé par les médias et les autorités politiques nationales et internationales, il est légitime de croire qu'un navire sans équipage est une prouesse technologique considérable visant à réduire l'accidentologie causée par l'Homme.

Statistiquement parlant, près de 80% des accidents maritimes sont liés à une erreur humaine[52]. En témoignent clairement les accidents de l'*"Amoco Cadiz"*ou du *"Mega Borg"*, causés par des erreurs humaines et dont les pertes

---

[49] VALERO C., TOURRET P., *" 20 ans d'apports des technologies aux industries maritimes"*, *op.cit.*, p.2.
[50] PIETTE G., Traité du Droit maritime, 2023, *op.cit.,* p.884.
[51] *Ibid.*
[52] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, *in.,* Transport et sécurité, LexisNexis, 2019, p.320.

étaient désastreuses[53]. Dès lors, le recours à l'utilisation des navires autonomes limitera certainement ces risques.

Toutefois et ce qui est aussi évident, l'habileté, la réactivité et l'improvisation que pourrait avoir l'être humain face à d'éventuelles situations d'urgence, ne seront jamais les points forts d'un navire sans équipage[54]. On se demande donc sur l'efficacité de l'intelligence artificielle (IA) à laquelle l'Humanité devient de plus en plus dépendante, face à des situations d'urgence imprévisibles, notamment dans le cas d'assistance en mer ou d'abordage.

Pour finir, il est essentiel d'aborder un autre aspect fondamental, celui du recours au connaissement électronique. Avec l'avènement du commerce électronique, il devient de plus en plus évident que l'utilisation de contrats numériques se généralise, en particulier dans le secteur maritime.

Aujourd'hui, la disparition progressive du recours au connaissement classique en papier a fait naître de nouvelles formes de livraisons de marchandises telle que la livraison par code Pin[55].

Or, avec la transition vers l'usage du connaissement électronique, une augmentation des risques de cybercriminalité a été constatée. L'affaire *MSC Mediterranean Shipping Company S.A. and Glencore International AG*[56] illustre bien ce risque. Il s'agit d'une jurisprudence anglaise, où le juge a refusé de considérer l'échange de code Pin comme un connaissement, en estimant que le manque de cyber vigilance et sécurité des systèmes informatiques de l'armateur, était la cause primaire de l'usurpation d'identité et du détournement des données, remis en question en l'espèce.

En somme, dans le monde maritime actuel, tout est devenu automatique. Une telle tendance est simplement une conséquence logique de la

---

[53] Pour plus de détails sur les pertes et indemnisations, *Cf., "Évaluation économique et indemnisation des dommages causés par les marées noires : enseignements tirés du cas de l'Amoco Cadiz"*, Archimer, IFREMER, https://archimer.ifremer.fr/.

[54] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, *op.cit.,* p.885.

[55] DIONE A.*, "L'assurabilité du connaissement électronique dans le cadre du transport maritime de marchandise",* Actualité juridique du village de la justice*,* https://www.village-justice.com/articles/*,* Consulté le 11/07/2023.

[56] Affaire de la Royal Courts of Justice Strand, *MSC Mediterranean Shipping Company S.A vs Glencore International AG,* London, WC2A 2LL, 24/05/2017, publié sur le site officiel de la cour, https://www .quadrantchambers.com/, Consulté le 11/07/2023.

mondialisation et de la numérisation croissante des flux commerciaux globaux. Par contre, ce qu'on trouve saillant, c'est que, souvent, les problématiques de cyber-sécurité sont délaissées dans la conception de ces systèmes informatiques[57]. Avec le développement continu de la technicité des logiciels utilisés à bord et dans les ports, le marin se trouve, aujourd'hui, face à de nouveaux risques immatériels et impalpables. Au regard de la complexité de ces moyens de technologie, les risques d'attaques, d'accidentologie et de pertes des navires connaissent une augmentation significative. La menace cyber, étant invisible, se nourrit essentiellement des manipulations erronées et des comportements frauduleux de la part des utilisateurs de ces technologies[58].

Par conséquent, tel que l'affirme Albert DIONE, *"la cybercriminalité abîme la confiance à la dématérialisation "*[59]. Ce caractère changeant et imprévisible explique la méfiance de la jurisprudence et de l'industrie d'assurance maritime face à la couverture de ces risques.

Pour leur part, il serait attendu des marins et, en général, des acteurs intervenant dans les opérations de transport maritime, qu'ils intègrent à leur vigilance, les risques associés à la manipulation des nouvelles technologies.

A cet égard, l'éveil et la sensibilisation à la gravité de ces menaces semble indispensable. Malheureusement, il a fallu du temps avant que l'ensemble des acteurs maritimes assimile cette réalité.

In fine, à l'ère d'une mondialisation constante, la démocratisation des nouvelles technologies et leur généralisation aux différents secteurs, continuent d'avoir d'importantes implications sur l'évolution des menaces, y compris dans le domaine du commerce maritime. Le cyber risque se présente, donc, comme l'un des ennemis les plus redoutés de l'industrie maritime. Perçu comme un risque *"caméléon",* la menace cyber est capable de prendre plusieurs formes et d'attaquer différentes cibles en même temps (B). D'où la difficulté de s'en prémunir et d'éviter sa multiplication

---

[57] BAUDU F., *"Les cyber-menaces contre les navires et les installations portuaires", op.cit.,* p.5.
[58] MANET F.-C., *"La marétique, un enjeu essentiel pour l'humanité ?"*, *op.cit.*, p.80.
[59] DIONE A., *"L'assurabilité du connaissement électronique dans le cadre du transport maritime de marchandise", op.cit.*

B)- La multiformité des menaces cyber dans le secteur maritime

Il suffit aujourd'hui de se rendre sur la passerelle d'un navire ou au centre de contrôle d'un port pour s'apercevoir que l'utilisation de l'informatique et des systèmes d'information dans le secteur maritime est de plus en plus répandue[60].

Il faut noter que la scène actuelle de l'industrie maritime poursuit son développement et s'appuie constamment aux technologies informatisées. En revanche, on manifeste un manque clair et net de conscience de la réalité de la menace cyber chez les opérateurs maritimes.

D'ailleurs, tel qu'il a été souligné en mai 2014 dans un article de Lloyd's List et selon le directeur de la protection de l'information au cabinet consultatif KPMG , *"...la cybersécurité à bord des navires marchands et dans les grands ports maritimes est en retard de 10 à 20 ans par rapport aux systèmes informatiques bureautiques, ce qui laisse la porte ouverte à une myriade de menaces de plus en plus redoutables"*[61]. Un décalage qui risque d'être irrattrapable face au rythme intensif avec lequel les nouvelles technologies numériques avancent.

Dans ce sens, la menace cyber en maritime peut prendre plusieurs formes. Selon le rapport du gouvernement français sur la cybersécurité maritime[62], le risque cyber peut se présenter sous la forme soit d'une menace externe, soit d'une attaque avec la mise en place d'un dispositif ou encore d'une menace interne.

---

[60] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"*, DMF n° 775, 8 décembre 2015, pp.1-2.

[61] Lloyds List, *"Shipping is 'decades behind' on cyber security, KPMG warns",* publié le 6 mai 2014 :, *"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"*, traduit par nous même, note (8), *in*., LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , DMF n° 775, 8 décembre 2015, p.5.

[62] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*, p.548.

Pour ce qui est des menaces externes, celles-ci sont causées principalement par des rançongiciels - *ransomware* ou par des attaques d'hameçonnage - *phishing* en anglais.

Le rançongiciel est défini comme étant "*...un programme informatique malveillant dont l'objectif est de chiffrer des données de manière à les rendre inaccessibles à leur propriétaire, puis demander à celui-ci, une rançon en échange de la clé qui permettra de les déchiffrer* "[63].

Dans la majorité des cas, ce logiciel malveillant se transmet par courriel via des pièces jointes ou des liens piégés. Une fois l'ordinateur en question est connecté au réseau, le ransomware va essayer de se diffuser et se propager dans d'autres systèmes d'informations[64].

Comme son nom l'indique, le but derrière un piratage par rançongiciel est de réclamer le versement d'une rançon, en échange de la clé de déchiffrement.

Bien que ce type d'attaque existait depuis nombreuses années, l'importance récente des crypto-monnaies a permis aux opérateurs criminels le paiement anonyme, ce qui laisse une porte ouverte à la multiplication de ce type de cyber menaces[65].

Dans cette optique, plusieurs entreprises ont subi de lourdes pertes suite à des attaques par rançongiciels.

A titre d'exemple, en 2021, le Swire Pacific Offshore[66], qui exploite une flotte de 50 navires, a été victime d'une attaque *ransomware*. Heureusement, bien que ce soit une perte importante pour l'entreprise et ses employés, aucun dommage matériel aux corps des navires n'a été enregistré. Certains analystes estiment que les données qui ont été volées comprenaient

---

[63] DREYFUSS M.-L., La révolution digitale dans l'assurance, *éd.*, L'Argus de l'assurance : les fondamentaux, 2018, p.66.

[64] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*, p.548.

[65] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ",* Thetius, Cyberowl, et HFW, 2022, p.12, traduit par nous même.

[66] *Cf.*, The Maritime Executive,*" Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data "*, publié le 26 novembre 2021, https://maritime-executive.com/article/ ransomware-attack-on-swire-pacific-offshore, Consulté le 14/07/2023.

notamment les passeports des employés, leur paie et des renseignements bancaires[67].

Quelques mois plus tôt, on a assisté à l'une des plus grandes attaques par rançongiciel. Elle concernait un pipeline colonial, un système d'infrastructures pétrolières fondamental aux États-Unis, allant de Houston à New York[68]. Environ 45% du carburant consommé sur la côte Est des États-Unis arrive via ce pipeline. En l'occurrence, les auteurs de cette attaque ransomware étaient des pirates russes, qui ont demandé 4.4 million de dollars en Bitcoin, pour rétablir le contrôle opérationnel à ces propriétaires[69].

Quant à l'hameçonnage ou le *phishing,* tel que défini par l'OMI dans le guide sur la cybersécurité au bord des navires, il s'agit du processus permettant au cybercriminel de tromper les destinataires pour qu'ils partagent des renseignements sensibles avec un tiers[70].

Autrement dit, le *phishing* est une technique par laquelle le cybercriminel envoie des courriels à un grand nombre de cibles potentielles demandant des données sensibles ou confidentielles particulières, telles que des données bancaires ou des mots de passe[71]. La victime reçoit un mail frauduleux qui l'invite à mettre à jour des informations personnelles sur un site falsifié. Une fois dessus, les données entrées par l'utilisateur seront collectées par le cybercriminel, qui n'a plus qu'à en faire usage[72].

L'hameçonnage peut aussi être ciblé. On parle en anglais de *spear phishing*. Dans ce genre de situations, le cybercriminel vise particulièrement une cible spécifique pour obtenir des informations sensibles, lui permettant

---

[67] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ", op.cit.*
[68] *Cf.,* The New York Times, "*Cyberattack Forces a Shutdown of a Top U.S. Pipeline",* publié le 08 mai 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline, Consulté le 14/07/2023.
[69]CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ", op.cit.*
[70] BIMCO, Guidelines on cybersecurity on board ship, 2020, glossary, *"Phishing refers to the process of deceiving recipients into sharing sensitive information with a third party*", p.59, traduit par nous même.
[71] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*, p.548.
[72] DREYFUSS M.-L., La révolution digitale dans l'assurance, *op.cit*., p.65.

d'accéder frauduleusement aux systèmes numériques de l'entreprise[73] . Si tel est le cas, le cybercriminel effectuera des recherches sur internet et sur les réseaux sociaux, pour *"... rendre le message plus crédible aux yeux du destinataire"*[74].

Enfin, tout comme en hameçonnage, en *spear-phishing* les personnes sont visées par des courriels personnels, qui contiennent souvent des logiciels falsifiés ou des liens qui téléchargent automatiquement des logiciels malveillants.

A ce titre, une étude du CESIN[75] de 2020 a souligné que le phishing et le spear-phishing prennent la tête des attaques, les plus couramment constatées dans le milieu maritime. D'ailleurs, en 2019, 79 % des entreprises piratées, ont témoigné avoir subi du phishing[76].

Pour ce qui est des attaques recourant dans leur fonctionnement à la mise en place de dispositifs malveillants, le gouvernement français, dans son rapport rédigé en 2022 sur la cybersécurité maritime, a souligné que, dans cette hypothèse, la menace cyber provient de l'installation de dispositifs techniques, facilement conçus par des informaticiens et permettant d'influencer rapidement des systèmes d'informations[77].

Le plus souvent dans ce cas de figure, ce sont des États belligérants désirant conduire des opérations de brouillage ou de leurre de signal GPS, dans des zones de conflits ou des zones maritimes assez fréquentées[78], qui recourent à cette technique d'attaque. Notons par exemple, le cas des Etats Unis qui ont reproché maintes fois à la Chine d'être derrière ces agressions[79].

---

[73] NOTIN J., *"Autopsie des cyberattaques et des moyens de s'en protéger par le dispositif national de prévention et d'assistance Cybermalveillance.gouv.frs", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.100.

[74] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*,p.548.

[75] CESIN : Club des Experts de la Sécurité de l'Information et du Numérique. Il s'agit d'un club réunissant des responsables de la cybersécurité venant d'entreprises de tous secteurs d'activités et d'administrations, ayant pour principal objectif de contribuer collectivement à la montée en maturité des organisations en cybersécurité. https://www.cesin.fr/.

[76] FRONCZAK S., *"Lutte contre la cybercriminalité maritime : Prévôts de la mer contre pirates", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.50.

[77] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*,p.548.

[78] *Ibid*.

[79] *Cf.,* Tradewinds, *" Sophisticated scams highlight growing cyber risk to shipping"*, publié le 10 octobre 2014, note (9), *in.* LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , *op.cit.*, p.2.

De même, en 2017, un *"wiper ware"*[80] destructeur lié à la Russie, connu sous le nom de *"NotPetya"*, a attaqué des entreprises autour du monde, causant des dommages et des interruptions d'activités estimés à 10 milliards de dollars, tel qu'expliqué dans un article du *Financial times* publié en 2022[81].

Aujourd'hui, avec la guerre en Ukraine, l'industrie d'assurance maritime s'inquiète davantage sur le risque de guerre cybernétique. Le conflit russo-ukrainien, et plus généralement les tensions géopolitiques actuelles ont refaçonné le paysage de la cybermenace[82].

A cet effet, la scène géopolitique présente a subi, à nouveau, une attaque par "*wiper ware",* connu sous le nom de *"IsaacWiper"*[83]*,* initiée par les autorités étatiques russes contre des services publics et organismes étatiques ukrainiens.

"Lancée une heure avant l'invasion, cette attaque a privé d'Internet un nombre d'entreprises et de services publics ukrainiens, mais aussi l'armée du pays, puis elle s'est propagée à de nombreux utilisateurs européens"[84].

A présent, le risque cyber s'impose davantage, de jour en jour, pour menacer également la souveraineté étatique. On parle d'arme cybernétique derrière laquelle se cachent même des Etats[85]. Dès lors, il faut admettre que le cyberespace est devenu un terrain de guerre comme tout autre[86].

---

[80] Un *"wiper ware"* est un type de *"malware"* : un logiciel malveillant conçu pour détruire et effacer les données, réseaux et fichiers pour toujours et parfois sans discrimination, traduit par nous même. Voir CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ",* Thetius, Cyberowl, et HFW, 2022, p.13.

[81] Financial Times, *"Insurers must rethink handling of cyber attacks on states"*, 29 aout 2022, note (18), *in.* Allianz Global Corporate & Specialty,*"Cyber: The changing threat landscape Risk trends, responses and the outlook for insurance"*, 2022, p.14.

[82] Allianz Global Corporate & Specialty,*"Cyber: The changing threat landscape Risk trends, responses and the outlook for insurance", op.cit.*

[83] *Cf.,* Palmer, ZDNet, *" Security researchers spot another form of wiper malware that was used against Ukraine's networks",* 2022, https://www.zdnet.com/article/security- researchers- spot-another-form-of-wiper -malware-that- was-used-against-ukraines-networks/, Consulté le 16/07/2023.

[84] Le Monde, *" La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques"*, 12 février 2023, https://www.lemonde.fr/economie/article/2023/02/12/la-guerre-en-ukraine-fait-basculer-le-monde-dans-l-ere-des -cyberattaques, Consulté le 16/07/2023.

[85] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , DMF n° 775, *op.cit.*, p.2.

[86] Le Monde, *" La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques"*, *op.cit.*

Pour ce qui est, maintenant, des menaces internes, celles-ci, peuvent être dues, soit à l'intervention du personnel employé, soit à un branchement au réseau[87].

Initialement, la menace peut être considérée comme interne si elle a pour source une mauvaise manipulation causée par des *"...utilisateurs qui ont un accès autorisé et légitime aux actifs d'une entreprise et qui en abusent, délibérément ou accidentellement"*[88].

Les cyberattaques de ce type peuvent être un acte intentionnel de la part d'un collaborateur ou un employé mécontent, pour le motif d'une vengeance personnelle, ou pour un motif financier ou encore, elle peut s'effectuer sous contrainte[89].

"Le comportement de ces personnes varie en termes de motivation, de sensibilisation, de niveau d'accès et d'intention"[90].

Par contre, le cas le plus fréquent, comme expliqué dans notre partie précédente, est essentiellement dû au manque de culture en cybersécurité. Les employés peuvent par exemple brancher une clé USB personnelle, non blanchie, ou installer des logiciels non professionnels[91], ce qui peut engendrer des attaques cyber.

La défaillance humaine est la principale cause des cyberattaques réussies. Par conséquent, la sensibilisation des acteurs de l'industrie maritime à l'importance de cette menace et l'impact que cela pourrait avoir, seront au cœur du dispositif de détection, de réaction et de préservation de la sécurité de l'organisation[92].

Ainsi, comme l'a indiqué, Jérôme Notin, directeur général de Cyber malveillance[93], on peut *"...s'être offert la plus belle porte blindée du monde, si on ne sait pas l'utiliser, on l'utilise mal, voire on laisse la porte ouverte, elle ne*

---

[87] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*,p.549.
[88] IBM, *" Pourquoi les menaces internes sont-elles particulièrement dangereuses ",* https://www.ibm.com/fr-fr/ topics/ insider-threats*,* Consulté le 16/07/2023.
[89] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime", op.cit.*, p.549.
[90] IBM,*" Pourquoi les menaces internes sont-elles particulièrement dangereuses ", op.cit.*
[91] *Ibid.*
[92] NOTIN J., *"Autopsie des cyberattaques et des moyens de s'en protéger par le dispositif national de prévention et d'assistance Cybermalveillance.gouv.fr", op.cit.,* p. 104.
[93] Cyber malveillance : outil national, mis en place par le gouvernement français, ayant pour mission d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cyber malveillance et de les informer sur les menaces numériques et les moyens de s'en protéger, https://www. cybermalveillance. gouv.fr/.

sera d'aucune utilité pour se protéger. C'est souvent partant de ce postulat que les attaquants pourront commettre leurs actions"[94].

Autrement dit et comme on l'a expliqué précédemment, la vigilance et la prudence dans l'utilisation de ces technologies est le seul moyen efficace pour se prémunir de ces attaques. La cybersécurité est tout d'abord une affaire de bon sens. On pourrait facilement éviter des cyberattaques si des mesures toutes assez simples étaient mises en œuvre, telles qu'une bonne gestion des mises à jour de sécurité, des sauvegardes et des mots de passe[95].

D'autre part, une menace interne pourrait également résulter d'une connexion à un réseau en compromettant des postes de travail ou en accédant aux systèmes informatiques de l'entreprise par des prises réseaux, situées dans des zones accessibles au public.[96]

Ce type de menace pourrait également compromettre la sécurité de nombreux systèmes, notamment d'autres cibles connectées à ce même réseau. A titre d'exemple, si un cybercriminel arrive à accéder au système d'information (SI) d'un navire, il serait capable d'atteindre le réseau de l'armateur qui lui, possède aussi l'accès au (SI) de ce navire[97].

A ce niveau, il est judicieux d'avouer qu'aujourd'hui, parallèlement à l'ingénuité et au développement des technologies numériques, les cybercriminels innovent constamment dans leurs menaces. Derrière la dématérialisation des procédures, peuvent se cacher parfois des intentions vicieuses, ayant pour but d'escroquer ou de frauder.

On parle notamment d'*arnaque au Président* par laquelle le cybercriminel sollicite les employés d'une société et demande un virement urgent et confidentiel en usurpant l'identité d'un dirigeant[98].

---

[94] NOTIN J., *"Autopsie des cyberattaques et des moyens de s'en protéger par le dispositif national de prévention et d'assistance Cybermalveillance.gouv.fr", op.cit.*, p.103.
[95] *Ibid.*
[96] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime", op.cit.*, p.549.
[97] *Ibid.*
[98] NOTIN J., *"Autopsie des cyberattaques et des moyens de s'en protéger par le dispositif national de prévention et d'assistance Cybermalveillance.gouv.fr", op.cit.*, p.101.

En résumé, il est clair qu'actuellement la menace cyber est un risque difficile à saisir. La multiformité des menaces et l'ingéniosité des pirates cyber dans leurs attaques, empêchent et freinent la possibilité d'y échapper totalement.

De surcroît, la multiformité des menaces est appuyée par une diversité d'auteurs et des motivations, ce qui rend encore plus difficile la tâche de se protéger contre les cyberattaques.

Dans ce sens, le centre canadien pour la cybersécurité, tel que rappelé par le professeur Gaëlle PIETTE, a classé six catégories d'auteurs de cyber-menaces avec autant de motivations. On trouve les Etats dont le motif est principalement géopolitique, les cybercriminels qui agissent avec un but lucratif, les hacktivistes dont le mobile est idéologique, les terroristes, les armateurs et enfin, les employés internes à une société éprouvant des sentiments de mécontentement[99].

En outre, la multiplicité des menaces, des auteurs et des motivations est également consolidée par une diversité de victimes. Avec la dématérialisation croissante dans le secteur maritime, aucune entité n'est à l'abri face à une menace cybernétique. Que ce soit la compagnie maritime elle-même, les navires en mer ou à quai, les ports, les cargaisons, voire même le personnel impliqué dans les opérations, tous sont susceptibles d'être ciblés par des cyberattaques.[100].

Tel que affirmé par Christian-Marc Lifländer, chef de la section cyberdéfense de l'Organisation du traité de l'Atlantique Nord (OTAN) au journal Le Monde,*"le cyberespace est un nouveau terrain de conflit. Il est désormais contesté et il le sera en permanence par des acteurs autoritaires qui testent nos limites"*[101]. Conséquemment, *"La menace doit être prise très au sérieux. Or, si celle-ci inquiète, un retard persiste dans ce domaine où la prise de conscience des acteurs ...prend du temps"*[102].

[99] PIETTE G., Traité du Droit maritime, 2023, *op.cit.,* p.539.
[100] *Ibid.*
[101] Le Monde, *" La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques"*, *op.cit.*
[102] COUSTILLERE A.,*"Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ?"*, RDNA, n°789, 2016/4, p.46.

En conclusion, cette nouvelle forme de piraterie représente des défis et des enjeux majeurs pour tous les acteurs du domaine maritime, ainsi que pour les États et les organisations internationales[103].

Protéger la marétique, à bord ou dans les ports, est une urgence devant l'imminence d'une menace multiforme aux conséquences potentiellement catastrophiques[104].

Cependant, le manque de considération quant à la gravité de ce risque est une problématique préoccupante qui nous pousse à contempler ses raisons (section 2)

[103] KERMARREC Y., *" Cybersécurité et monde maritime : contexte, enjeux, challenges et opportunités",* DMF, nº 842, 1er janvier 2022, p.5.
[104] BAUDU F.*, "Les cyber-menaces contre les navires et les installations portuaires",* Gazette n°43, CAMP, 2017, p.6.

Section 2 : Prise de conscience tardive de la nécessité de couvrir le risque cyber maritime

La prise de conscience de la nécessité de couvrir le risque cyber maritime a été lente à émerger, mais, à présent, elle devient de plus en plus prégnante, depuis que le secteur maritime subit l'impact grandissant des cyberattaques.

Initialement, les acteurs du domaine maritime ont souvent sous-estimé les risques liés à la numérisation et à l'automatisation croissante de leurs opérations. Les menaces cybernétiques sont longtemps passées inaperçues ou ont été reléguées au second plan, laissant le secteur vulnérable à de potentielles attaques.

La cybermenace représente un défi sans précédent pour le secteur maritime, car elle introduit des risques complexes et récents, pour lesquels les acteurs de l'industrie n'avaient pas été préparés auparavant. La nouveauté de cette menace a pu entraîner une réticence initiale des assureurs à proposer des solutions de couverture. Une méfiance justifiée par la nature particulière de ce risque (A).

Cependant, à mesure que les cyberattaques augmentent en fréquence et en gravité dans le secteur maritime, la perception de la couverture du risque cyber évolue (B). Les acteurs de l'industrie prennent conscience de l'importance critique de la cybersécurité et commencent à chercher des solutions d'assurance pour se protéger contre les cyberattaques.

A)- La nature particulière du risque cyber, raison primaire de son appréhension

Les échanges commerciaux par voie maritime constituent la majorité du trafic du commerce mondial. Toutefois, face à la dépendance croissante de ce secteur aux technologies numériques dans la gestion de la navigation, la logistique et les communications... , tout dysfonctionnement de ces systèmes risque d’avoir des conséquences graves sur l’ensemble des flux commerciaux internationaux.

Concrètement, une cyberattaque maritime aboutie peut entraîner des perturbations massives dans les chaînes d'approvisionnement internationales, ce qui, par conséquent, entraînera un bouleversement de l'économie mondiale.

Dans ce sens, la nature spécifique du risque cyber rend la tâche de s'en prémunir encore plus ardue. Les particularités de cette menace se manifestent à différents niveaux.

Tout d'abord, identifier ou définir clairement ce que peut représenter un risque cyber n'est pas une mission aussi simple. Tel qu'exposé précédemment, la nouveauté de ce risque et la multiplicité des menaces, des auteurs et des cibles cybers, compliquent la possibilité d'avoir une vue exhaustive sur ce qui peut être perçu comme cybermenace maritime.

Dans le but d'essayer de rassembler la panoplie de ces risques, plusieurs institutions nationales et internationales essaient de les délimiter. A titre d'exemple, le centre canadien pour la cybersécurité les considèrent comme étant l'ensemble des : *"...activités qui visent à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient"*[105].

Le BIMCO, à son tour, propose une définition aussi générale du risque cyber. Citée dans les directives sur la cybersécurité et la cyber sûreté à bord des navires, la menace cyber peut être identifiée comme *"un événement qui, dans les faits ou potentiellement, peut avoir des conséquences négatives sur le système embarqué, le réseau et l'ordinateur ou les informations qu'ils traitent, stockent ou transmettent, et peut nécessiter une intervention pour atténuer les conséquences*"[106].

Ainsi, l'absence de définition universelle faisant l'unanimité démontre clairement la méconnaissance du cyber risque par les différents acteurs maritimes et non maritimes[107]. Par ricochet, ces difficultés éprouvés à délimiter

[105] Définition du centre canadien pour la cybersécurité, *in.*, PIETTE G., Traité du Droit maritime, 2023, *éd.,* Pedone, p.538, note (11).

[106] Les directives sur la cybersécurité et la cyber sûreté à bord des navires – publiées par BIMCO, l'Association internationale des lignes de croisière (CLIA), la Chambre internationale de la marine marchande (ICS), l'Association internationale des transporteurs de marchandises solides (INTERCARGO) et l'Association internationale des armateurs pétroliers indépendants (INTERTANKO), Glossary, p. 58. Traduit par nous même.

[107] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.69-70.

clairement la menace cybernétique, auront indéniablement une influence sur sa prise en charge par les assureurs[108].

Ensuite, la singularité de la menace cyber réside essentiellement dans l'éventualité qu'elle soit un risque potentiellement systémique[109]. Tel que souligné par le Ministère de l'économie, de l'industrie et de l'emploi, une menace systémique est perçue comme étant un *"...risque de dégradation brutale de la stabilité financière, provoqué(e) par une rupture dans le fonctionnement des services financiers, et répercuté(e) sur l'économie réelle"*[110].

En d'autres termes, une menace est dite systémique si elle est issue d'un même fait générateur, capable d'impacter plusieurs acteurs distincts et attaquer différentes cibles, ce qui va diminuer l'aléa et plaider pour sa non-assurabilité[111].

Bien qu'il soit récent, le risque cyber a cette capacité de s'étendre largement et de s'étaler sur un ensemble de systèmes[112].

En maritime, les technologies informatiques sont majoritairement interconnectées. Elles jouent un rôle essentiel dans la coordination et l'articulation entre les différentes infrastructures, telles que les ports, les navires, les compagnies maritimes, les chargeurs de marchandises, les banques, etc.

De ce fait, une cyberattaque sur un maillon de la chaîne peut se propager rapidement à l'ensemble des structures, engendrant de graves pertes et dommages directs et indirects.

A titre d'illustration, dans l'hypothèse d'une cyberattaque systémique réussie dans le secteur maritime, des dégâts importants liés à la restauration des systèmes, des pertes de revenus due à des arrêts de service et des dommages à la réputation des entreprises maritimes, peuvent être mis en cause. Outre les dommages financiers, une cyberattaque maritime peut également entraîner des

---

[108] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.,* p.70.
[109] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , DMF, n°842, 01 janvier 2022, p.1.
[110] LEPETIT J.-F., "*Rapport sur le risque systémique"*, Ministère de l'Economie, de l'Industrie et de l'emploi, avril 2010, p. 12.
[111] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , *op.cit.,* p.1.
[112] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, p.18.

risques environnementaux tels que le déversement de produits chimiques ou de pétrole en raison d'un contrôle défaillant des navires.

D'ailleurs, selon un rapport de 2020 publié par le Carnegie Dotation pour la paix internationale, le risque cybernétique présente un potentiel élevé pour les pertes agrégées ou regroupées, et un seul événement cybernétique peut entraîner des réclamations d'indemnisation de sources multiples[113]. L'étude a également assimilé les pertes systémiques causées par les cyberattaques à celles provoquées par les catastrophes naturelles[114]. Tel qu'il figure dans l'annexe 3, les pertes financières causées, en 2017, par la NotPetya cyberattaque, par exemple, s'élèvent à 10 milliards de dollars, ce qui est très proche des dommages subis suite à l'ouragan Irene en 2011.

Dans ce même esprit, l'office comptable du gouvernement américain a souligné que les préoccupations au sujet des risques systémiques découlant des cyberattaques poussent davantage les assureurs à chercher à modéliser les pertes au-delà des dommages financiers connus et non catastrophiques, pour les inclure dans le modèle des répercussions des cyber événements catastrophiques[115]. Ce qui explique davantage la réticence de l'industrie d'assurance maritime quant à la couverture de ces risques.

La banque de France, à son tour, a rappelé que selon une enquête sur le risque systémique menée en 2019 par la Banque d'Angleterre, 61% des participants ont éprouvé des inquiétudes quant à l'impact des cyberattaques sur le système financier, les plaçant devant le risque géopolitique et le risque d'un ralentissement économique mondial[116]. Elle a aussi affirmé que le risque cyber n'est clairement plus un risque opérationnel idiosyncratique ; il devient désormais potentiellement systémique[117].

---

[113] BATEMAN J., *"War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*", Carnegie Endowment for International Peace, p.7.
[114] Voir annexe 3, p.112.
[115] United States Government Accountability Office, Report on CYBER INSURANCE : *"Insurers and Policyholders Face Challenges in an Evolving Market"*, May 2021, p.20. Traduit par nous même.
[116] Banque de France, Une mesure de l'évolution du risque cyber, Billet n°246, 17 décembre 2021.
[117] *Ibid.*

En résumé, l'impact de ces attaques ne se limite plus à la gestion de la perte ou du vol de données dans le seul secteur maritime. *"Les atteintes à la propriété, à la réputation, ainsi qu'aux coûts liés à la perte d'exploitation…"*[118] inquiètent également l'ensemble des intervenants dans ce domaine.

A la lumière de ces constatations, le comité Européen des risques systémiques attire l'attention sur la nécessité de prendre conscience de l'ampleur, la rapidité et le rythme de propagation potentiels d'un cyber incident majeur et appelle les autorités concernées à prendre des réponses efficaces afin d'atténuer les effets négatifs éventuels sur la stabilité financière[119]. En réponse, de nombreux assureurs, tel que *CHUBB insurance*, invitent également à s'adapter à cette particularité, vu qu'il s'agit d'un risque qui a le potentiel d'infliger des dommages étendus en raison de points communs ou d'éléments partagés en matière de risque[120].

Aujourd'hui, l'industrie assurantielle se trouve face à une augmentation des risques systémiques. Dès lors, le secteur d'assurances maritimes est mis à l'épreuve en raison de la multiplication des catastrophes naturelles, des bouleversements causés par la pandémie du Covid-19 sur l'économie mondiale et la montée en agressivité et en sophistication des cyberattaques.

Alors que la France est arrivée enfin à sortir de l'épisode catastrophique de la pandémie du Covid 19, la viabilité du système assurantiel français est mise au défi face à la recrudescence des risques systémiques, en particulier celui du dérèglement climatique, à l'origine de catastrophes naturelles, dont les conséquences sont les plus graves, suivi en deuxième position, du risque cyber, selon le baromètre des risques 2022 d'Allianz France[121].

---

[118] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.,* p.71.
[119] Recommandation du comité Européen du risque systémique, Sur un cadre paneuropéen de coordination des cyber incidents systémiques pour les autorités concernées, (CERS/2021/17), 02 décembre 2021, (4).
[120] *Cf.,* CHUBB , *"Cyber Systemic Risk/Product Update: broker FAQs",* https:// www.chubb.com/ content/dam/chubb-sites/chubb-com/fr-fr/campagne-digitale/cyber/FAQ-courtiers-risques.
[121] Avis, Conseil économique, social et environnemental, *"Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques"*, JORF, avril 2022, p.4.

Le plus inquiétant des scénarii pour l'industrie d'assurance serait le cas où ces trois menaces systémiques se produisent simultanément au cours d'une même période. Hypothèse qui n'est pas du tout écartée, étant donné que ces trois risques sont souvent interdépendants.

D'ailleurs, pas plus que l'an dernier, nous avons été témoins de l'impact que la crise sanitaire a pu avoir sur l'usage des technologies de l'information et de la communication, et qui a entraîné un accroissement des cyberattaques et une amplification du dysfonctionnement des infrastructures numériques[122]. *"A ces risques dont l'ampleur est inédite, s'ajoutent ceux liés au dérèglement climatique qui génère des modifications irréversibles de nos écosystèmes"*[123].

M. Nassim Taleb, dans son ouvrage *"The Black Swan"*[124]classe ces risques en deux catégories : des *"cygnes noirs"* et des *"cygnes verts"*. Le concept de *"cygne noir"* ou *"black swan"* est défini comme un événement imprévisible qui peut avoir des conséquences considérables. Il se distingue par trois caractéristiques : il est inattendu, rare, ayant un impact extrême. Les attentats terroristes ou la crise du coronavirus sont des exemples clairs de *"black swans"*. Quant aux risques liés au changement climatique, ceux-ci sont plutôt des *"cygnes verts"*, vu qu'ils sont de plus en plus prévisibles[125].

La cybermenace, elle par contre, est l'un de ces événements imprédictibles qui peuvent avoir un impact important sur les individus, les organisations et les nations entières, et donc peut être qualifiée comme *"cygne noir"*.

Au cours de ces dernières années, nous avons assisté à plusieurs cyberattaques qui ont perturbé les entreprises et les gouvernements du monde entier. Le piratage SolarWinds en est l'illustration, où une cyberattaque

[122] Avis, Conseil économique, social et environnemental, *"Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques", op.cit.*, p.6.
[123] *Ibid.*
[124] *Cf.,* TALEB N., The Black Swan: The Impact of the Highly Improbable, Random House, 2007.
[125] Avis, Conseil économique, social et environnemental, *"Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques", op.cit.,* p.25.

sophistiquée a compromis les systèmes de multiples organismes gouvernementaux et entreprises privées[126].

Aujourd'hui, la menace cyber représente la troisième économie mondiale, après les Etats unis et la Chine, ce qui est équivalent à 6 000 milliards d'euros environ et qui devrait atteindre en 2025, 10 500 milliards de dollars[127].

En 2020, les cyberattaques ont représenté 217 millions d'euros d'indemnisation, en forte hausse par rapport à 2019, en raison du recours massif à internet durant les phases de confinement et au télétravail, comme décidé par les pouvoirs publics pendant la pandémie[128].

La croissance du commerce électronique pendant la pandémie a conduit également à une crise du transport maritime conteneurisé, durant laquelle, la Chine a fermé ses ports et a arrêté la fabrication des conteneurs.

Tous ces facteurs démontrent davantage, l'interdépendance de ces risques systémiques.

Dans les faits, les grands armateurs possèdent des réseaux mondiaux d'une ampleur considérable, où le numérique joue un rôle essentiel dans leur fonctionnement. Les ports, quant à eux, représentent des structures complexes, rassemblant de nombreux acteurs, et nécessitent une interconnexion des systèmes pour garantir à la fois la sécurité et l'efficacité dans un environnement hautement concurrentiel, où les flux logistiques sont soumis à une forte pression[129].

D'où, une augmentation de la demande en commerce international, telle que vécue lors de la pandémie, augmentera sans doute les risques cybers, d'autant plus que les flux commerciaux internationaux se basent majoritairement sur le trafic maritime.

---

[126] CentralEyes, *"The Top Cybersecurity Breaches in the UAE"*, May 16th 2022, https://www .central eye.com/ the-top-cybersecurity-breaches-in-the-uae/, Consulté le 29/07/2023. Traduit par nous même.

[127] CIO Letter, *"Cyber, de la sécurité à la résilience",* mai 2022, p.2. https://alternativeviews.tikehaucapital. com/ sites/tikehau-cap-blog/files/CIO%20Letter/CIO-Letter-FR.pdf, Consulté le 29/07/2023.

[128] Avis, Conseil économique, social et environnemental, *", op.cit.,* p.12.

[129] JACQ O., *"Les perspectives en matière de réglementation et de bonnes pratiques en cybersécurité maritime"*, DMF, n°842, 1er janvier 2022, p.1.

De même, si on était face à une catastrophe naturelle. Dans ce cas, les risques de fausses alertes et de diffusions d' informations erronées seraient beaucoup plus élevés.

Pour faire face à ces défis interconnectés, il est essentiel que l'industrie maritime adopte une approche holistique et coordonnée. Cela implique qu'il faut absolument investir dans la cybersécurité pour protéger les infrastructures critiques, renforcer la résilience des opérations face aux pandémies et aux catastrophes naturelles, ainsi que s'engager dans des pratiques durables pour contribuer à atténuer les effets du dérèglement climatique. A cet effet, la collaboration entre les acteurs de l'industrie, les gouvernements et les organismes internationaux reste essentielle pour élaborer des stratégies et des politiques efficaces visant à prévenir et à gérer ces risques interconnectés.

Personne ne nie que la nature particulière du risque cyber et notamment ses caractères potentiellement systémiques et cumulatifs peuvent engendrer des difficultés dans le calcul des volumes de primes nécessaires et des indemnisations[130].

Toutefois, si l'industrie assurantielle joue pleinement son rôle et couvre, même partiellement, ces menaces, elle serait un véritable amortisseur des chocs économiques consécutifs, malgré leur imprévisibilité et l'étendue de leur impact[131].

Pour conclure, la cyber menace systémique dépend essentiellement de deux facteurs : une dépendance technologique forte et une interconnexion accrue. Ces deux aspects augmentent indubitablement les portes d'entrée des virus[132].

De ce fait, l'éventualité d'un *"cyber ouragan"* ou d'un risque cyber systémique, passant par des failles des systèmes informatiques ou par des "chevaux de Troie"[133], est incontestablement en train de s'intensifier. La

[130] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , *op.cit.,* p.3.
[131] Avis, Conseil économique, social et environnemental, *op.cit.*, p. 7.
[132] *Cf.,* rapport de l'Institut Montaigne, *"Cybermenace : avis de tempête"*, novembre 2018.
[133] *"Le salarié est souvent le maillon faible de la cybersécurité, voire un « cheval de Troie »", in.,* Rapport d'information du Sénat français relatif à la cybersécurité des entreprises, n°678, 10 juin 2021, p. 10.

fragilité systémique de nos économies contribue sans doute à l'amplification de la menace cyber[134].

Enfin, même les grands fournisseurs d'accès, souvent en situation de monopole, ceux qu'on croyait invincibles, sont régulièrement attaqués et ne sont pas immunisés contre ce risque. La cyberattaque contre Microsoft Exchange en début mars 2021, ayant affecté 60 000 entreprises, l'a clairement démontré[135].

Il est évident qu'à présent nous sommes à l'orée d'une nouvelle époque où les risques cyber sont non seulement plus globaux mais aussi de plus en plus interconnectés[136].

Néanmoins, bien que *"...nous sommes devenus intolérants au risque[137] , nous ne faisons pas toujours tout ce qu'il faut pour nous en couvrir ni nous en préserver : notre acculturation au risque cyber (information, sensibilisation, précaution) reste insuffisante"[138]*. Il a fallu attendre la multiplication et l'aggravation des cyberattaques et leur impact financier de plus en plus étendu, sur l'industrie maritime pour en prendre conscience (B).

[134] Rapport de l'institut Montaigne, *"Cybermenace : avis de tempête",* novembre 2018, p.12.
[135] Rapport d'information du Sénat français relatif à la cybersécurité des entreprises, n°678, 10 juin 2021, p.109.
[136] Avis, Conseil économique, social et environnemental, *op.cit*., p. 7.
[137] HEIDERICH D., "*Risques majeurs : les prévenir, les gérer"*, président de l'Observatoire international des crises, L'abécédaire des institutions , 09 novembre 2021, *in.*, Avis, Conseil économique, social et environnemental, *op.cit*., p.7 , note(6).
[138] Avis, Conseil économique, social et environnemental, *op.cit*., p. 7.

B)- L'aggravation des cyber-attaques, une alerte pour l'industrie maritime

Ces dernières années, le monde maritime a connu une nette augmentation des attaques cyber, entraînant une évolution inquiétante des pertes associées (1). En conséquence, la recrudescence de ces attaques a suscité une prise de conscience urgente au niveau mondial. Face à la gravité de ces menaces, la communauté internationale a reconnu la nécessité d'une réponse concertée et a collaboré étroitement pour développer des mesures préventives et des réglementations spécifiques afin de mieux protéger l'industrie maritime contre cette menace grandissante (2).

1. L'accentuation de la menace cyber sur le secteur maritime

Suite en partie à plusieurs attaques très médiatisées, la perception des cyberrisques dans l'industrie maritime a évolué au cours des dernières années. Il y a à peine cinq ans, l'industrie du transport maritime était considérée comme une cible improbable pour les pirates cyber[139].

Ce n'est qu'en 2011 que le Bureau Maritime International (BMI) a finalement alerté contre la croissance exponentielle des cyber attaques maritimes. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a confirmé la gravité de la situation dans son rapport sur la sécurité maritime. Ce rapport mettait en évidence le niveau de protection insuffisant des infrastructures maritimes et portuaires face aux potentielles cyberattaques[140].

"Un exemple fort connu est la cyberattaque dont le port d'Anvers a été victime en 2011"[141]. En l'occurrence, *"...l'un des plus grands ports d'Europe a été le théâtre d'un piratage informatique orchestré par un cartel de trafiquants de drogue. Le groupe aurait embauché un pirate informatique pour*

[139] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ",* Thetius, Cyberowl, et HFW, 2022, p.10. Traduit par nous même.
[140] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.71-72.
[141] PIETTE G., Traité du Droit maritime, 2023, *éd.,* Pedone, p.538.

cibler les agents portuaires, infecter le système d'information du port et récupérer un mot de passe d'accès au système de gestion des conteneurs"[142].

La base de données qui a été compromise, contenait des renseignements précis sur l'emplacement de chaque conteneur dans le port. Parallèlement, ces trafiquants de drogue, tenus au courant de la localisation exacte des conteneurs, faisaient entrer et sortir régulièrement des stupéfiants, emballés dans des conteneurs chargés de bois et de bananes, pendant au moins deux ans[143].

L'opération a été si efficace et discrète que les chargeurs réels de la cargaison n'en sont pas rendus compte, étant donné que leurs marchandises étaient restées intactes. Les autorités portuaires ne l'ont pas su non plus, jusqu'à ce que les criminels deviennent très avides de gain et commencent à retirer des conteneurs entiers du port, ce qui mène finalement à la découverte de l'opération[144]. En l'espèce, les cybercriminels ont eu recours à des chevaux de troie et des keyloggers[145].

Ces menaces sur les ports n'étaient pas du tout sporadiques. D'autres infrastructures portuaires ont été pareillement ciblées. A titre d'exemple, en septembre 2019, le port de de Barcelone et de San Diego ont fait l'objet d'attaques cybernétiques[146].

Outre les infrastructures portuaires, les compagnies maritimes ont également été ciblées par ces attaques. Ces dernières représentent une menace sérieuse pour les entreprises maritimes, vu qu'elles peuvent entraîner des conséquences graves sur leurs opérations, leur sécurité et leur réputation.

A ce titre, selon une étude intitulée "Data Breach Digest", réalisée par Verizon, une compagnie maritime a été victime d'une série d'actes de piraterie en mer, rendus possibles par une intrusion dans ses systèmes informatiques[147]. Les pirates ont réussi à pénétrer à bord en utilisant des boîtiers à lecteur de

[142] COUSTILLERE A.,*"Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ?"*, RDNA, n°789, 2016/4, p.45.
[143] CHUBB N., FINN P., et NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ",* Thetius, Cyberowl, et HFW, 2022, p.11, traduit par nous même.
[144] *Ibid.*
[145] *Le keylogger* est un logiciel espion qui identifie notamment les touches utilisées par une personne sur son clavier d'ordinateur. Il permet ainsi de récupérer des identifiants et des mots de passe, *in.*, PIETTE G., Traité du Droit maritime, *op.cit.*, p.538, note (14).
[146] PIETTE G., Traité du Droit maritime, *op.cit.*, p.538.
[147] COUSTILLERE A.,*op.cit.*, p.45.

codes-barres pour localiser et dérober des caisses de grande valeur et leur contenu[148].

Quant aux attaques par rançongiciels, devenues de plus en plus fréquentes en transport maritime, un changement de tactique à été aperçu chez les cybercriminels dans deux domaines qui devraient être particulièrement préoccupants pour l'industrie maritime[149].

Le premier changement de tactique concerne le ciblage et les objectifs des cyber pirates. Ils visent désormais des systèmes qui intègrent une technologie opérationnelle, pour causer une défaillance physique de l'équipement, parfois critique pour la sécurité. C'était notamment le cas de l'attaque sur le pipeline pétrolier colonial, fondamental aux États-Unis, exposée précédemment et qui a causé des pertes financières énormes à son propriétaire[150].

Vient en deuxième lieu, mais tout aussi préoccupant, le deuxième changement de tactique. Désormais, les auteurs de menaces de ransomware ciblent de plus en plus les organisations s'occupant de la chaîne d'approvisionnement pour ensuite compromettre et extorquer leurs clients. D'ailleurs, en 2021, les attaques contre la chaîne d'approvisionnement ont triplé. On cite notamment, les attaques très médiatisées contre *SolarWinds* et *Kaseya*[151], des fournisseurs de logiciels qui sont souvent utilisés par des propriétaires et des exploitants de navires, ou d'autres organisations de la chaîne d'approvisionnement maritime[152].

A ce niveau, il importe de noter que les attaques les plus dangereuses ont été menées non pas par des cybercriminels mais plutôt par les Etats. Alors que les criminels commettent une part importante d'attaques, les États ont la

---

[148] COUSTILLERE A.,*op.cit.*, p.45.
[149] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry "*,*op.cit*., p.12. Traduit par nous même.
[150] *Ibid*.
[151] *Cf.,* Cybernews, *"Opinion : Kaseya has dealt with cyberattack better than SolarWinds"*, 28 septembre 2021. https://cybernews.com/security/opinion-kaseya-has-dealt-with -cyberattack -better -than- solarwinds/, Consulté le 30/07/2023.
[152] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry "*, *op.cit*.

capacité de piloter des attaques beaucoup plus sophistiquées avec une étendue de dommages plus large.

C'était le cas notamment, comme évoqué précédemment, du *wiper ware*, "*IsaacWiper",* ou de plusieurs autres attaques réussies lancées par la Russie et ciblant spécifiquement les institutions ukrainiennes. Contrairement aux ransomwares conçus pour crypter les systèmes, puis les déchiffrer une fois la rançon payée ; les logiciels malveillants "*Wiper"* sont inventés pour détruire les données pour toujours.

La plus importante cyberattaque, par "*Wiper"*, et la plus célèbre, dans le milieu maritime reste celle de *NotPetya* en juin 2017, touchant le groupe AP Moller-Maersk lui causant des pertes de plus de 300 millions de dollars[153] et plus de 3 milliards de dollars américains à l'industrie d'assurance, selon *PCS Global Cyber*[154]. Il a fallu plusieurs jours à Maersk Line pour reconstruire son réseau, dont le coût estimatif au début se situait entre 200 millions de dollars américains et 300 millions de dollars américains en pertes de revenus. FedEx lui aussi ayant subi des dommages suite à cette attaque, a estimé les coûts à 400 millions de dollars américains[155]. Quant à *Mondelez International*, il a réclamé 100 millions de dollars américains, mais son assureur a refusé de l'indemniser au motif que l'événement était un acte de guerre[156].

Deux ans plus tard, le ransomware *LockerGoga*[157] a frappé une série de cibles énergétiques et industrielles, paralysant leurs systèmes. Six entreprises ont été touchées, avec une perte totale assurée à l'échelle de l'industrie d'un peu plus de 100 millions de dollars américains, tel que l'a souligné *PCS Global Cyber Data*, mais, en réalité les pertes économiques étaient encore plus élevées[158].

---

[153] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.71.
[154] MICAN A., *" Cyber and infrastructure chokepoints", in.*, IUMI Eye Newsletter, mars 2022, p.19.
[155] FedEx Corporation Annual Report, FedEx, 2019, *in.*, CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry "*,*op.cit*., p.13, note (10). Traduit par nous même.
[156] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry "*,*op.cit*., p.13. Traduit par nous même.
[157] *Cf.,* Axa insurance-reinsurance website,*"The LockerGoga Ransomware Attack: A worst-case scenario for industrial operations",* 03 juin 2019, https://axaxl.com/fast-fast-forward/articles /the -lockergoga- ransomware -attack_a-worst-case-scenario-for-industrial-operations, Consulté le 30/07/2023.
[158] MICAN A.,*"Cyber and infrastructure chokepoints", op.cit.*

Enfin, depuis 2017, la cadence des cyberattaques s'est accélérée : Mærsk (2017), COSCO (2018), Carnival (2019), l'Organisation Maritime Internationale - OMI, MSC, CMA CGM et Hurtigruten (tous en 2020)[159].

Par ailleurs, si ces cyberattaques visent avant tout les compagnies maritimes et les infrastructures portuaires, à terre, *"...la sophistication des outils employés permet, dorénavant, de cibler les navires en mer, pouvant aller jusqu'à leur détournement"*[160].

La cybermenace continue d'évoluer et, à l'heure actuelle, les infrastructures essentielles sont devenues encore plus vulnérables, en partie, à cause des deux années complètes de pandémie mondiale.

Pendant le coronavirus, on a vécu une augmentation énorme des cyber attaques, ce qui a laissé certains parler de *"cyber ouragan"* touchant de multiples acteurs.

Loin d'être une pure invention de l'esprit, ce type d'attaques, tel qu'on a pu le voir, et comme il est clair à partir de l'annexe 4[161], existe et entraîne de lourdes pertes financières[162].

A présent, les navires sont également fréquemment piratés, à raison d'un navire par jour[163]. Multiples sont les cas comprenant un incident, au cours duquel des arpenteurs de soutes de navires accèdent aux ordinateurs, dans une salle de contrôle des moteurs, pour imprimer des documents, à partir d'une clé USB, qui introduit un virus dans le système. Dans d'autres situations, les navires perdent leur réseau ECDIS[164], à cause d'un virus et doivent donc recourir à des chartes en papier[165].

---

[159] PIETTE G, *" Le commerce maritime face au risque cyber"*, DMF, n°842, 01 janvier 2022, p.1.
[160] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.71.
[161] Voir annexe 4, p.112.
[162] Rapport de l'institut Montaigne, *"Cybermenace : avis de tempête",* novembre 2018, p.17.
[163] OSLER D., *"One ship is hacked everyday on average",* Lloyds list, 06 juillet 2021, p.1.
[164] L'ECDIS (Electronic Chart Display Information System) est un système de cartes électroniques, qui permet de visualiser en temps réel la position du navire sur une carte présentée sur un écran. Ce système permet de se passer de cartes papier, *in.,* PIETTE G., Traité du Droit maritime, *op.cit.*, p.539, note (16).
[165] OSLER D., *"One ship is hacked everyday on average", op.cit.*

Dès lors, "*...la cyber menace n'est plus un risque émergent ; c'est un risque immédiat qui nécessite au moins une solution émergente "*[166].

Pour les acteurs de l'industrie maritime, il est crucial aujourd'hui de savoir comment protéger leurs opérations contre les attaques ciblées et les menaces virulentes provenant de l'écosystème numérique interne ou externe.

Comprendre ce qui rend l'industrie particulièrement vulnérable est essentiel pour surmonter les petites failles dans les systèmes informatiques qui peuvent entraîner des pertes inimaginables[167].

En résumé, compte tenu de l'aggravation des pertes et des dommages causés par les cyberattaques sur le plan économique mondial, y compris dans le domaine maritime, la société internationale a pris conscience de l'urgence d'agir pour limiter l'impact de ces menaces croissantes. Pour faire face à cette problématique complexe, des règles juridiques spécifiques ont été instaurées (2).

2. L'accentuation de la menace cyber sur le secteur maritime

Selon le "Doyen Carbonnier" et tel qu'affirmé dans son ouvrage *La sociologie juridique de 1978,* le droit n'est pas seulement un objet de transmission, de compréhension et d'analyse, mais aussi un moyen d'action sur le monde et un reflet de celui-ci[168]. La sociologie législative est ainsi nécessaire afin d'établir des règles juridiques efficaces. Elle nous permet de comprendre comment le droit émerge des interactions sociales et comment il influence à son tour les comportements et les relations entre les individus.

A l'évidence, le droit suit les faits sociaux, puisqu'il puise sa légitimité et son efficacité dans la réalité changeante de la société. Cette logique s'applique *mutatis mutandis* en Droit maritime.

---

[166] MICAN A., *" Cyber and infrastructure chokepoints", in.*, IUMI Eye Newsletter, mars 2022, p.19. Traduit par nous même.

[167] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry "*, *op.cit*., p13.

[168] Commentaire *"Sociologie Juridique, chapitre 1 - Jean Carbonnier (1978) - La sociologie juridique avant le XXe siècle"*, https://www.doc-du-juriste.com/droit-prive-et-contrat/droit-civil/commentaire-de-texte/sociologie-juridique-chapitre-1-jean-carbonnier-1978-sociologie-juridique-avant-siecle, Docs du juriste, Consulté le 05/08/2023.

Personne ne peut nier *"...que le droit maritime est un droit de commerçants, né de la pratique. Face à l'émergence d'une cyber-criminalité, l'industrie a su réagir en créant une "soft law", reprise dans une "hard law" constituée par des textes réglementaires d'origine nationale ou internationale*"[169].

A cet égard et afin d'avoir un aperçu général synthétique, il est pertinent de présenter les règles juridiques traitant ce sujet, adoptées aux niveaux national, régional et international universel.

Sur le plan national, la France était précurseur en la matière. Depuis 2008, le Livre blanc sur la Défense et la Sécurité nationale[170] "*...avait déjà souligné la nécessité d'élaborer une doctrine en la matière"*[171] et de mettre en place une agence chargée de la sécurité des systèmes d'information (ANSSI).

En 2013, le livre blanc, dans sa nouvelle version, a fixé les règles officielles en matière de cybersécurité et a créé le concept d' Opérateurs d'Importance Vitale[172] (OIV) et la notion de Systèmes d'Information d'Importance Vitale (SIIV), dont les secteurs des transports et de l'industrie en font partie, depuis 2016[173].

Dans ce sens, la Direction des Affaires Maritimes et l'ANSSI ont édicté trois guides[174] : *"Cyber-sécurité – évaluer et protéger le navire"*[175],

---

[169] LOOTGIETER S., *"Cyber-sécurité et Transport maritime"*, Gazette n°43, CAMP, 2017, p.3.

[170] Livre blanc, Défense et sécurité nationale, 2013. http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

[171] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.72.

[172] *"Les Opérateurs d'Importance Vitale (OIV) sont les opérateurs qui exploitent les installations indispensables à la vie du pays. Ils sont désignés par le ministère coordonnateur selon une procédure interministérielle. On compte 12 Secteurs d'Activité d'Importance Vitale (SAIV) répartis en 4 groupes : l'activité humaine (alimentation, gestion de l'eau, santé), l'activité régalienne (activités militaires, judiciaires, civiles de l'État), l'activité économique (énergie, finances, transports) et l'activité technologique (communications, audiovisuel, industrie, espace et recherche)"*, *in*., Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *éd.*, 2022, p.557, note (33).

[173] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.72.

[174] LOOTGIETER S., *"Cyber-sécurité et Transport maritime",op.cit.,* p.3.

[175] Guide Direction des Affaires Maritimes, Cybersécurité évaluer et protéger le navire, septembre 2016, https://goo.gl/OWmf2N, consulté le 05/08/2023.

"*Guide des bonnes pratiques de sécurité à bord des navires"*[176] et *"Cybersécurité – renforcer la protection des systèmes industriels du navire"*[177]. Ces guides mettent l'accent sur l'importance pour les compagnies maritimes et les équipages de respecter une certaine *"hygiène informatique"* ou encore d'installer des *"outils de sécurisation"* nécessaires pour identifier le cyber-risque et en limiter ses conséquences[178].

D'un autre côté, l'arrêté du 23 novembre 1987 relatif à la sécurité des navires, prévoit, depuis 2016, dans son article 130.39, *"Règles relatives au matériel de sûreté",* que l'évaluation de sûreté du navire doit traiter des dispositions relatives à sa cybersécurité[179].

"*Le texte fournit trois éléments sur lesquels l'évaluation doit, au minimum, se prononcer : la cartographie logicielle et matérielle du navire, la définition des éléments sensibles de ce dernier, (et) la gestion des vulnérabilités système"*[180]. L'évaluation doit aussi consigner de manière formelle les mesures prises par la compagnie maritime pour protéger les systèmes de communication et d'information au niveau du plan de sûreté du navire[181].

Finalement, au niveau national, il convient d'évoquer le rôle particulièrement structurant qu'a eu l'article 22 de la Loi de Programmation Militaire (LPM) 2014-2019[182]. Ces dispositions ont permis de délimiter les exigences associées aux enjeux de sécurité informatique pour les 250 Opérateurs d'Importance Vitale (OIV) en France[183].

Quant au niveau régional Européen, plusieurs structures ont été mises en place dans le but de renforcer la cybersécurité dans l'espace communautaire.

---

[176] L'ANSSI, Guide des bonnes pratiques de sécurité informatique à bord des navires, mars 2015, https://goo.gl/ kS p rgG, Consulté le 05/08/2023.

[177] Guide Direction des Affaires Maritimes, Cyber sécurité- renforcer la protection des systèmes industriels du navire, janvier 2017. https://goo.gl/yv5EN9, Consulté le 05/08/2023.

[178] LOOTGIETER S., *"Cyber-sécurité et Transport maritime",op.cit.,* p.3.

[179] Arrêté du 23 novembre 1987 relatif à la sécurité des navires et à la prévention de la pollution, Article 130.39. V. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000841523, Consulté le 07/08/2023.

[180] PIETTE G., Traité du Droit maritime, 2023, *op.cit.,* p.541.

[181] *Ibid.*

[182] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. V. https://www.legifrance. gouv.fr/ jorf/article_jo/JORFARTI00002833890, Consulté le 07/08/2023.

[183] JACQ O., *"Les perspectives en matière de réglementation et de bonnes pratiques en cybersécurité maritime"*, DMF, n°842, 1er janvier 2022 , p.1.

Le premier pas dans la stratégie de cybersécurité communautaire a été la création de l'agence européenne, chargée de la sécurité des réseaux et de l'information (ENISA) en 2004, dont le siège est situé en Grèce[184].

L'Agence s'engage à établir des systèmes de certification en matière de cybersécurité pour renforcer la fiabilité des nouvelles technologies de l'information et de la communication.

Elle collabore également avec les États membres et les organes de l'Union européenne pour renforcer la résilience de leurs infrastructures et garantir la sécurité numérique des citoyens[185].

A côté de l'ENISA, on trouve une deuxième structure européenne spécialisée en cybersécurité, tout récemment fondée. Il s'agit du centre européen de compétence en matière de cybersécurité (ECCC), créé en 2021[186].

Ce dernier *"...vise à renforcer les capacités et la compétitivité de l'Europe en matière de cybersécurité"*[187]. Il oeuvre principalement à : premièrement, la mise en place et l'aide à la coordination du réseau des centres nationaux de coordination et la communauté de compétences en matière de cybersécurité[188], ensuite, la prise de décisions stratégiques en matière d'investissement et la mise en commun des ressources de l'Union européenne, de ses États membres et de l'industrie[189], et enfin, la mise en œuvre d'un soutien financier lié à la cybersécurité[190] au titre du programme Horizon[191] Europe et des programmes pour une Europe numérique[192].

---

[184] LASMOLES O., *"Cybersécurité et navires sans équipage"*, DMF, n°817, octobre 2019, p.775.
[185] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*, p.554.
[186] Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.
[187] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime"*, *op.cit.*, p.554.
[188] *Ibid.*
[189] *Ibid.*
[190] *Ibid.*
[191] *"Horizon Europe est le programme-cadre de l'Union européenne pour la recherche et l'innovation pour la période allant de 2021 à 2027. Le programme Horizon Europe prend la suite du programme Horizon 2020 qui s'est terminé à la fin de l'année 2020"*, *in.*, Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*, p.554, note (23).
[192] Le programme Europe numérique 2021-2017 vise à soutenir et accélérer la transformation numérique de l'économie, de l'industrie et de la société européenne*, in., ibid.,* p.554, note (24).

Ces structures ont permis d'élaborer un corpus juridique important en matière de cybersécurité sur le plan communautaire.

A ce titre, nous citons dans un premier temps, la directive n° 2016/1148 du 6 juillet 2016, concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne[193]. Cette directive a été le premier texte d'envergure, adopté au sein de l'Union Européenne (UE), sous l'égide de l'ENISA[194].

Elle impose à ses États membres certains objectifs, notamment celui d'adopter une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, tel qu'il est clair des dispositions de l'article 14 alinéa 1 de la directive : "*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*".

Notons que ladite directive a été transposée, en Droit français, par la loi n° 2018-133 du 26 février 2018[195] et le décret du 23 mai 2018[196].

Par le biais de la directive, on a également créé une nouvelle catégorie d'opérateurs : les opérateurs de services essentiels (OSE).

Tel que évoqué par le Pr. Lasmoles, pour être classé OSE, trois critères sont nécessaires : d'abord, l'entité doit fournir un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques.

[193] 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.
[194] LASMOLES O., *"Cybersécurité et navires sans équipage"*, DMF, n°817, octobre 2019, p.775.
[195] Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772, Consulté le 05/08/2023.
[196] 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, JORF, 25 mai 2018, p. 1.

Ensuite, la fourniture de ce service doit être tributaire des réseaux et des systèmes d'information et enfin un incident sur cette entité doit avoir un effet disruptif important sur la fourniture dudit service[197]. "*En étant désignée OSE, l'entreprise a des obligations telles que l'application de règles de sécurité aux systèmes d'information essentiels qu'elle a préalablement identifiés"*[198] ou la notification incidents de sécurité survenus sur ses Systèmes d'Information Essentiels à l'ANSSI[199].

Par ailleurs, dans la continuité de la directive NIS 1, la directive NIS2[200] adoptée le 10 novembre 2022, est considérée comme extrêmement ambitieuse. *"Face à des acteurs malveillants toujours plus performants et mieux outillés, touchant de plus en plus d'entités trop souvent mal protégées, la directive NIS 2 élargit, en effet, ses objectifs et son périmètre d'applicabilité pour apporter davantage de protection"*[201]. Cette extension du périmètre prévue par NIS 2 est sans précédent en matière de réglementation cyber.

Elle devrait entrer en vigueur en France, au second semestre de l'année 2024[202].

Dans un second temps, un autre texte important mérite d'être mentionné. Il s'agit du Règlement européen du 17 avril 2019, surnommé le Cybersecurity Act[203]. Ce dernier poursuit deux objectifs : *" (1) renforcer et asseoir le rôle et les attributions de l'Agence européenne pour la cybersécurité (ENISA) et (2) fixer des règles de certification commune, en vue de créer un*

---

[197] LASMOLES O., *"Cybersécurité et navires sans équipage"*, DMF, n°817, *op.cit.* p.776.
[198] *Ibid.*
[199] *Ibid.*
[200] NIS 2, Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, https:/ /eur-lex.europa.eu/legal-content/FR/TXT, Consulté le 05/08/2023.
[201] ANSSI, *"Directive NIS 2 : Ce qui va changer pour les entreprises et les administrations françaises"*, publié le 17/01/2023, Consulté le 05/08/2023.
[202] *Ibid.*
[203] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE), no 526/2013, (règlement sur la cybersécurité), https://digital-strategy.ec.europa.eu/en/policies/ cybersecurity-act, Consulté le 05/08/2023.

marché unique numérique pour les produits, services et processus liés aux technologies de l'information et de la communication"[204].

En d'autres termes, cet acte établit un cadre de certification en cybersécurité, ayant pour but de promouvoir l'intégration de la sécurité dès la conception - *security by design* et d'imposer par défaut des paramètres les plus sécurisés.

En dernier lieu, il nous semble fondamental d'évoquer le Règlement Général sur la Protection des Données (RGPD) qui a été publié le 4 mai 2016[205]. Celui-ci constitue la pierre angulaire en matière de préservation des données personnelles, en optant pour l'accompagnement des administrations ainsi que les entreprises dans ce domaine[206].

Dans le cadre du RGPD, les organismes sont tenus de nommer un délégué à la protection des données (DPO) afin d'assurer un niveau de sécurité adapté aux risques. Chaque pays doit mettre en place une structure de contrôle local, œuvrant dans ce sens. En France, il s'agit de la Commission Nationale de l'Informatique et des Libertés (CNIL)[207].

Par ailleurs, 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"*.

En pratique, les analyses d'impact relatives à la protection des données (AIPD), imposées par le RGPD, compliquent la mission de couverture de ce risque par les assureurs. Ces derniers concernés au premier degré par le

[204] PIETTE G., *"Le commerce maritime face au risque cyber"*, DMF, n° 842, 1er janvier 2022, p.1.
[205] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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), https://eur-lex. europa.eu/legal -content/FR/TXT, Consulté le 05/08/2023.
[206] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*, p.556.
[207] *Ibid.*

traitement de données à caractère hautement personnel, ont du mal à se conformer aux dispositions du RGPD, particulièrement, à l'article précité.

"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"[208].

En dernier lieu, et sur un niveau international plus large, d'autres textes ont été adoptés.

Le premier texte international universel à évoquer ce sujet, était la convention de Budapest du 23 novembre 2001 portant sur la cybercriminalité[209].

Ce traité international à l'initiative du Conseil de l'Europe, sert de référence pour tout pays qui développe une législation complète en matière de lutte contre la cybercriminalité, tout en fournissant un cadre pour la coopération internationale entre les États parties concernés[210].

A travers ce texte, le Conseil de l'Europe cherchait à établir *"un cadre complet et cohérent en matière de cybercriminalité et de preuves électroniques*"[211]. Le but principal derrière son adoption était d'exiger des Etats parties à adopter les textes nécessaires pour ériger les infractions liées à la cybercriminalité en infraction pénale dans leur ordre juridique[212].

En France, cette convention a été adoptée par le biais du décret n°2006-580 du 23 mai 2006[213].

A présent, le Conseil de l'Europe publie périodiquement des notes explicatives et des guides portant sur divers aspects de la Convention.

Il met aussi en place des réunions entre les Etats signataires dans le cadre des Conférences Octopus qui permettent à ces États de dresser un bilan sur la situation des menaces[214].

---

[208] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, p.27.
[209] Conseil de l'Europe, Convention sur la cybercriminalité, Budapest, 23.XI.2001, Série des traités européens - n° 185, https://rm.coe.int/168008156d, consulté le 06/08/2023.
[210] Convention de Budapest, Dépliant sur les avantages de la Convention de Budapest, Version 19 avril 2023, https://rm.coe.int/cyber-buda-benefits-19april-2023-fr/1680aafa6f, consulté le 06/08/2023.
[211] *Ibid.*
[212] PIETTE G., Traité du Droit maritime, *op.cit.*, p.540.
[213] Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, JORF, 24 mai 2006.
[214] LASMOLES O., *"Cybersécurité et navires sans équipage"*, DMF, n°817, *op.cit.* p.777.

Sous l'égide de l'Organisation Maritime Internationale (OMI), la réglementation en matière de cybersécurité maritime peut être répartie en instruments juridiques contraignants et normes plus souples, sous forme de recommandations.

Pour ce qui des recommandations, l'OMI a publié d'abord les Directives sur la gestion des cyber-risques maritimes, (MSC-FAL.1/Circ.3)[215].

"Ces directives fournissent des recommandations de haut niveau sur la gestion des cyber-risques maritimes visant à protéger les transports maritimes contre les cybermenaces et vulnérabilités actuelles et émergentes. Elles comprennent également les éléments fonctionnels sur lesquels repose une gestion efficace des cyber-risques"[216].

Plus tard, le conseil de la sécurité maritime (MSC) de l'OMI a adopté, le 16 juin 2017, la résolution MSC (428)[217]. Celle-ci a constitué une étape fondamentale dans l'acculturation du transport maritime aux enjeux de cybersécurité[218].

D'emblée, elle a clôturé le débat entre les partisans de l'inclusion de la question de cybersécurité maritime au code ISPS[219], donc la rattachant à la sûreté maritime, et ceux qui supportent sa liaison au code ISM[220], pour une gestion plus large de sécurité[221]. L'ensemble des acteurs maritimes se sont, alors, trouvés dans des terres moins inconnues[222].

---

[215] IMO, Guidelines on cyber risk management, https://wwwcdn.imo.org/localresources/en/OurWork /Facilitation/ Facilitation/MSC-FAL.1-Circ.3-Rev.1% 20-%20Guidelines%20 On% 20 Maritime % 20 Cyber%20Risk%20Management%20(Secretariat).pdf, Consulté le 07/08/2023.
[216] OMI, site officiel, https://www.imo.org/fr/OurWork/Security/Pages/Cyber-security.aspx, Consulté le 07/08/2023.
[217] Résolution MSC.428(98), sur la Gestion des Cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité (SGS), https://wwwcdn.imo.org/ localresources/fr/OurWork /Security/Documents/ MSC% 20 98-23-Add.1.pdf, Consulté le 07/08/2023.
[218] BANITZ L., *"Les cyber risques dans le monde maritime : de la prise de conscience aux actes"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p. 25.
[219] OMI, Code international pour la sûreté des navires et des installations portuaires (ISPS), entré en vigueur le 1er juillet 2004.
[220] OMI, Le Code international de gestion de la sécurité (Code ISM), résolution A.741(18), entré en vigueur le 1er juillet 1998.
[221] BANITZ L., *"Les cyber risques dans le monde maritime : de la prise de conscience aux actes"*, *op.cit.*, p. 25.
[222] *Ibid.*

La résolution incite également les administrations *"... à contrôler la cybersécurité maritime de leur système de gestion de sécurité (SGS)*[223] *au plus tard lors de la première vérification annuelle de l'attestation de conformité de la compagnie après le 1er janvier 2020"*[224].

Quant aux instruments obligatoires, adoptés au sein de l'OMI et régissant, en partie, la problématique de la cybersécurité maritime, nous trouvons, dans un premier temps, le code ISPS (International Ship and Port Facility Security), traitant de la lutte contre le terrorisme dans le monde maritime.

Depuis 2002, ce texte faisait déjà référence à la sécurité des systèmes d'information et des réseaux[225] et exigeait des transporteurs maritimes de mettre en place des mesures de protection physique des systèmes d'information du navire[226].

De son côté, le code international de gestion de sécurité (ISM) a servi également de support en matière de cybersécurité maritime.

Introduit en 1994 dans la Convention pour la sauvegarde de la vie humaine en mer (SOLAS)[227] au chapitre IX « Gestion pour la sécurité de l'exploitation des navires », *"...ce code vise à renforcer la sécurité des transports maritimes internationaux et à mettre en œuvre un cadre international pour la sécurisation de la gestion et de l'exploitation des navires"*[228].

Le *International Safety Management* code, impose alors aux transporteurs maritimes de rédiger "*... une politique compagnie sur les*

[223] Selon les termes de la résolution MSC.428(98), un SGS est approuvé si les cyber-risques sont gérés conformément aux objectifs et exigences du code international de gestion de sécurité (ISM), V. Le gouvernement Français, Secrétariat général de la mer, *"Cybersécurité maritime"*, L'économie bleue en France, éd. 2022, p.550.

[224] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *éd,.* 2022, p.550.

[225] JACQ O., *"Les perspectives en matière de réglementation et de bonnes pratiques en cybersécurité maritime"*, DMF, n°842, 1er janvier 2022 , p.1.

[226] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.72.

[227] OMI, Convention Internationale pour la sauvegarde de la vie humaine en mer (SOLAS), signée à Londres le 20 janvier 1914. http://archive.org/details/textofconvention00inte/ page/ n5/mode/ 2up? view=theater, Consulté le 08/08/2023.

[228] Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *op.cit.*, p.551.

systèmes d'information du navire et de contrôler les échanges des systèmes d'information du navire"[229].

Ayant fait le tour des différents textes juridique régissant la question de cybersécurité maritime, et bien qu'ils soient nombreux et constructifs, ces textes demeurent clairement inadaptés aux cyber risques maritimes actuels[230]. Ce qui explique, d'ailleurs, les initiatives prises par les associations et les organismes non gouvernementaux dans le but de lutter contre la cybercriminalité maritime, tel que le BIMCO, qui a adopté, en 2016, un guide sur la cybersécurité à bord des navires[231].

A présent, l'OMI, à travers les recommandations susmentionnées, le travail régulier du comité maritime international (CMI) et en particulier l'activité de son groupe de travail, *Cybercrime in shipping*[232], traite régulièrement du sujet et essaie de trouver les solutions idoines pour faire face à la menace cybernétique en maritime[233].

En guise de conclusion de ce chapitre, il est important de souligner qu'aujourd'hui, face à la multiplication des cyberattaques, plusieurs entreprises de grande envergure commencent à adopter des politiques positives, allant vers le sens de la cyber résilience, et oeuvrent, de plus en plus, à la mise en place des dispositifs de défense sophistiqués, pour compliquer la tâche aux cybercriminels.

Cependant, cette prise de conscience de l'importance de la cyberdéfense, constatée au sein des grandes entreprises, a impacté négativement les petites entreprises et a réorienté ces menaces vers les entreprises, les plus vulnérables, qui n'ont pas les moyens de se protéger.

---

[229] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.72.
[230] *Ibid.*, p.73.
[231] BIMCO, Guidelines on cybersecurity on board ships, https://www.bimco.org/about-us-and-our-members/publications /the-guidelines-on-cyber-security-onboard-ships, Consulté le 08/08/2023.
[232] Cybercrime in shipping est un groupe de travail sur la cybercriminalité dans le transport maritime du CMI. Il a été formé suite à la conférence de New York en 2016, au cours de laquelle une session informative a été organisée sur le sujet. L'objectif initial du groupe était de surveiller et de rechercher ce domaine crucial du transport maritime et ses effets sur les aspects juridiques. V. https://comitemaritime.org/work/cybercrime/.
[233] PIETTE G., Traité du Droit maritime, *op.cit.,* p.541.

C’est dans ce sens que plusieurs auteurs estiment que, *“ L’effet domino peut être dévastateur”*[234].

A cet effet, la cybersécurité doit être l’affaire de tous et de toute la chaîne de valeur[235]. Elle reste avant tout *“...la défense en profondeur des systèmes et des organisations face au risque numérique : une seule barrière n'est jamais suffisante pour réduire suffisamment un risque. C'est la multiplication des barrières, organisationnelles, technologiques, opérationnelles, humaines et la recherche de la résilience qui permettra de limiter réellement les impacts”*[236].

Enfin, ce qui est aussi marquant, c’est qu' aucun de ces différents textes n’a abordé le sujet d’assurabilité du risque cyber maritime.

Nous verrons dans notre second chapitre, que la réponse à cette question n’était pas du tout évidente. Les controverses persistent encore autour du risque cyber maritime, même quand il s’agit de sa couverture en assurance (CHAPITRE 2ème).

.

[234] Rapport d’information du Sénat français relatif à la cybersécurité des entreprises, n°678, 10 juin 2021, p. 10.
[235] *Ibid.*
[236] JACQ O., *“Les perspectives en matière de réglementation et de bonnes pratiques en cybersécurité maritime”*, *op.cit.* , p.1.

CHAPITRE 2ème - Réponse de l'industrie d'assurance maritime face au risque cyber

Tel que souligné dans le chapitre précédent, l'étude des cybermenaces et de leur impact sur l'industrie du transport maritime démontre que le risque de cyberattaque constitue une véritable entrave à la croissance de cette industrie, d'autant plus qu'elle devient de plus en plus automatisée.

Dans ce sens, une étude hypothétique, dirigée par le projet *Cyber Risk Management (CyRiM)*, une initiative publique-privée, basée à Singapour, qui évalue les cyberrisques, dont Lloyd's est l'un des membres fondateurs[237], apporte la preuve des conséquences catastrophiques qu'une attaque cyber-systémique pourrait avoir sur les principaux ports d'Asie-Pacifique.

Dans ce rapport, on décrit un scénario plausible, sous le nom de "*Shen Attack",* selon lequel une attaque, lancée via un virus informatique, transporté par des navires, brouille les enregistrements de la base de données de fret dans les 15 principaux ports d'Asie-Pacifique et entraîne de graves perturbations[238].

Dans un tel scénario, l'ampleur de l'attaque causerait des dommages économiques considérables à un large éventail de secteurs d'activité à l'échelle mondiale en raison de l'interconnectivité de la chaîne d'approvisionnement maritime[239]. L'annexe 5[240] illustre clairement cette interconnexion.

Tel qu'on peut voir sur cette carte, ce *malware* hypothétique aurait un impact important sur divers pays tiers, qui seraient touchés dans l'ensemble de leur chaîne d'approvisionnement. Le niveau 1 (tier 1) montre les pays

[237] *Cf.,* CyRiM (Cyber Risk Management), *"Shen Attack: Cyber Risk in Asia Pacific Ports",* 2019, https://assets .lloyds.com/assets/pdf-cyrim-shen-attack-final-report/1/pdf-cyrim-shen-attack-final-report.pdf, Consulté le 09/08/2023.
[238] Lloyds, *"Shen Attack: Cyber risk in Asia Pacific ports"*, 14 octobre 2019, https://www.lloyds.com/news-and-insights/ risk-reports / library/shen-attack-cyber-risk-in-asia-pacific-ports, Consulté le 09/08/2023.
[239] *Ibid.*
[240] Voir annexe 5, p.113.

directement visés par ce virus. Dans ce scénario, il s'agirait du : (Japon, Malaisie, Singapour. Le deuxième niveau (orange) affiche les cinq principaux partenaires commerciaux de chacun des pays touchés, y compris les États-Unis et la Chine. Les pays du niveau 3, comme le Canada, le Mexique et l'Inde, sont les cinq principaux impactés, suite à leur partenariat commercial maritime, avec les pays du niveau 2, et ainsi de suite[241].

Enfin, on estime que, dans ce genre de situation, les pertes peuvent aller jusqu'à 110 milliards de dollars[242], si ce virus affecte 15 ports de l'Asie-Pacifique.

Aujourd'hui, il est incontestable que cette dépendance accrue aux nouvelles technologies numériques, dans le secteur maritime, influence majoritairement la recrudescence de la menace cyber et entraîne comme partout ailleurs, des conséquences financières de l'ordre de milliards de dollars[243].

A ce niveau, l'industrie d'assurance maritime ne peut rester insensible au risque cybernétique. Au contraire, dans le cas où une entreprise est victime d'un sinistre quelle qu'il soit, le fait de se diriger vers son assureur, est une conséquence naturelle et attendue. "*Les choses ne sont pas différentes lorsque ce sinistre a été causé par une attaque cybernétique* "[244].

Il faut admettre que la scène actuelle démontre que la sensibilisation et l'éducation sur la cybersécurité au sein de l'industrie maritime restent à améliorer.

Dès lors, *"la prévention, malheureusement, ne suffit pas toujours"* et c'est là qu'intervient l'assureur maritime pour protéger les acteurs maritimes d'éventuelles pertes et couvrir les potentiels risques cyber.

---

[241] CyRiM (Cyber Risk Management), "*Shen Attack: Cyber Risk in Asia Pacific Ports"*, 2019, https://assets. lloyds. com/assets/pdf-cyrim-shen-attack-final-report/1/pdf-cyrim-shen-attack-final-report.pdf. p.21, Consulté le 09/08/2023.
[242] Lloyds, *"Shen Attack: Cyber risk in Asia Pacific ports"*, 14 octobre 2019, *op.cit.*
[243] Adam Assurances, *"Les menaces cyber dans le secteur maritime: a-t-on déjà envisagé tous les scénarios ?*", Le Lab – Recherches et innovations en assurances maritimes et transport, 20 avril 2020, p.1.
[244] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"*, DMF n° 775, *op.cit.*, p.3.

Sur le front de l'assurance, l'offre de couverture pour les risques cyber maritimes est encore en train de se développer. Un état des lieux de celle-ci serait, alors, essentiel pour comprendre son évolution (section 1).

L'assurance sert, d'emblée, à combattre l'aléa et prévoir les futurs risques. Par conséquent, elle devra s'acclimater au progrès technologique rapide et au changement continu des menaces, afin de rester en phase avec les nouveaux défis.

A cet effet, l'avenir du marché de l'assurance du risque cyber maritime résidera dans son aptitude à innover, à s'adapter aux évolutions technologiques et à satisfaire les différents acteurs maritimes, en leur offrant des solutions complètes et adéquates, face à des menaces cybernétiques de plus en plus sophistiquées (section 2).

Section 1 : Etat des lieux sur la couverture assurantielle du risque cyber maritime

L'aléa est un déterminant fondamental de l'assurabilité d'un risque. Ce dernier peut être couvert, s'il existe une incertitude dans sa réalisation. Par ailleurs, une entreprise peut choisir de transférer ce risque à des assureurs dès lors qu'elle pourrait avoir des difficultés à financièrement l'assumer en cas de réalisation[245]. "*Le risque cyber maritime peut être considéré comme entrant dans la catégorie des risques transférables"*[246]. Toutefois, la scène actuelle d'assurance cyber maritime est encore en pleine phase d'évolution.

Initialement, la couverture en assurance du risque cybernétique était exclue des polices d'assurance (A). Par la suite, avec l'évolution des menaces et la recrudescence des attaques, la protection assurantielle se révèle essentielle pour limiter les dommages et préserver l'ensemble de la chaîne d'approvisionnement (B).

[245] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, DMF n°842, 01 janvier 2022, p.1.
[246] *Ibid.*

A)- Le principe : L'exclusion du risque cyber dans les polices maritimes

De prime abord, le caractère potentiellement systémique du risque cyber maritime, sa nouveauté et sa capacité à engendrer des accumulations de pertes à la charge des assureurs, ont plaidé pour son exclusion des polices assurantielles maritimes.

Certes, le développement de l'importance des systèmes d'information sur la navigabilité des navires et sur les activités des compagnies maritimes a poussé le marché d'assurance maritime, à s'interroger sur l'éventualité de garantir ce risque[247]. Mais, très vite, cette industrie s'est montrée sceptique et a choisi de ne pas le couvrir, afin d'éviter des pertes financières considérables.

Cette perspective est exprimée manifestement à travers les clauses d'exclusion du risque cyber (1) incorporées dans les polices d'assurance maritime. Mais, également, d'une façon indirecte, à travers son assimilation à des risques déjà exclus des polices maritimes (2).

1. Des clauses d'exclusion spécifiques au risque "marétique" :

Très tôt, l'assurance a pris en considération les préjudices, découlant des risques cybernétiques, mais, initialement, c'était, dans le but de les exclure de la couverture des risques ordinaires[248].

En effet*, "l'évolution de la technologie utilisée a créé un aréopage de causes nouvelles auxquelles le marché de l'assurance maritime a répondu par la prudence et la mise en place de la clause dite 380"*[249].

Sur la base de la clause 380, aussi appelée "*Institute Cyber Attack Exclusion clause",* les cybercrimes sont explicitement exclus des polices d'assurance maritime.

[247] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.*, p.1.
[248] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"*, *op.cit.*, p.3.
[249] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.*, p.1.

Cette clause stipule, dans un premier temps, que la police d'assurance *: "...ne couvre en aucun cas la responsabilité ou les dépenses liées aux dommages causés directement ou indirectement par, ou résultant de l'utilisation ou de l'exploitation, comme moyen d'infliger un préjudice, de tout ordinateur, système informatique, programme informatique, code malveillant, virus ou processus informatique ou tout autre système électronique"*[250].

Par contre, dans le cas où elle serait entérinée dans une police spécifique au risque de guerre ou tout autre risque comparable, cette clause couvre les pertes résultant de l'utilisation des technologies numériques, dans le système de lancement et/ou de guidage et/ou le mécanisme de tir de toute arme ou missile[251].

Cette exclusion, nous la trouvons, notamment, dans la couverture des P&I Clubs. *"Certains vont reprendre mot à mot la clause 380"*[252]. Dans ce sens, il faut noter que les P&I Club prévoient également des clauses spécifiques sur le connaissement électronique et excluent sa couverture *"...dans le cas où le mécanisme électronique permettant d'utiliser les documents n'a pas été approuvé préalablement par le club de protection"*[253].

En janvier 2012, cette clause additionnelle a été transposée en Droit français, dans la police française d'assurance maritime sur corps de navire en prévoyant que : *"sont exclus les pertes et dommages, recours de tiers ou dépenses résultant directement ou indirectement de*[254]*l'utilisation ou de l'exploitation, avec l'intention de causer des dommages, de tout ordinateur ou équipement informatique, programme ou logiciel informatique, programme*

---

[250] Institute Cyber Attack exclusion clause : *"1.1…in no case shall this insurance cover loss damage liability or expense directly or indirectly 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"*. Traduit par nous même.

[251] Institute Cyber Attack exclusion clause : *"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 or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile"*

[252] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , *op.cit.,* p.3.

[253] *Ibid.*

[254] Souligné par nous même.

malveillant, virus informatique ou processus informatique, ou tout autre système électronique "[255]

Attachée aux polices d'assurance maritime *corps*, la clause 380 sert à protéger les assureurs, face à un péril considéré comme non maritime[256].

Le caractère large de l'exclusion est visible à travers l'utilisation des termes : *"résultant directement ou indirectement de"*. La formulation de cette clause met en exergue les énormes efforts, soumis lors de la rédaction, pour s'assurer que l'élimination de la couverture de ce risque soit générale[257].

Dans ce sens, plusieurs auteurs, tel que Baris Soyer, estiment que, même dans le cas, d'un dommage collatéral, résultant d'un acte ne visant pas directement la chose assurée, cette clause est susceptible d'être appliquée[258].

Dans ce même ordre d'idées, l'interprétation de cette clause dans les polices d'assurance maritime, se base généralement sur la notion de *proxima causa*, c'est-à-dire l'événement considéré comme fait générateur du dommage, est celui le plus près dans le temps de la réalisation du préjudice[259].

Donc, grâce à la clause 380 et son côté très large d'exclusion, les assureurs n'auront qu'à démontrer une *remote cause* ou une cause distante du dommage, pour pouvoir échapper à la couverture du risque cyber maritime[260].

Néanmoins, la clause 380 de 2003, n'est pas aussi claire ni exhaustive, comme on le pensait à l'origine. Il est d'ailleurs admis que celle-ci ne vise que les dommages matériels. Cependant, dans le monde du transport maritime, les dommages physiques causés par une cyberattaque restent rares[261].

---

[255] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , *op.cit.*, p. 2.
[256] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.*
[257] KAO M.-B., *"Cybersecurity in the Shipping Industry and English Marine Insurance Law"*, Tulane Maritime Law Journal, vol. 45, no. 3, summer 2021, p.486.
[258] SOYER B., *"Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems", in.*, New Technologies, Artificial intelligence and shipping law in the 21st Century, *éd.,* Ban Soyer & Andrew Tettenbom, 2019, p.636, *in.,* KAO M.-B., *"Cybersecurity in the Shipping Industry and English Marine Insurance Law"*, *op.cit.,* p.486.
[259] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.* p.2.
[260] *Ibid.*
[261] Astaara Co. Limited, *"LMA 5403, a lost opportunity ?"*, juillet 2020, https://astaaragroup.com/ wp-content/ uploads/2020/07/LMA-5403-A-Lost-Opportunity.pdf , p.3, Consulté le 12/08/2023.

En outre, la clause 380 reste, également, silencieuse s'agissant de savoir si l'intention de viser l'assuré doit être démontrée. De nombreuses attaques cybernétiques étaient globales sans cibles précises ni déterminées. Ainsi, demeure la question de savoir si l'exclusion de la clause 380 peut être appliquée en l'absence d'une intention de causer des dommages au navire assuré[262].

De même, cette clause a pu susciter des réflexions quant à l'inclusion d'une *silent cyber cover*, soit une couverture silencieuse potentielle d'un risque cyber qui n'a pas été expressément exclu. Autrement dit, la clause 380, malgré sa généralité, ne soustrait pas de manière adéquate, toutes les expositions à cette menace, notons par exemple le cas des menaces non ciblées. Par conséquent, il y a potentiellement lieu d'une couverture cyber silencieuse résiduelle, qui entraîne une incertitude quant à l'étendue de l'exclusion[263].

Enfin, à mesure que les attaques augmentent en nombre et en sophistication, l'inadéquation de l'utilisation de la CL380 devient de plus en plus claire[264]. *"Le temps était donc venu de clarifier la volonté des assureurs et d'adapter l'achat de couvertures d'assurance à ce nouveau risque"*[265].

"...Le risque cybernétique étant de plus en plus important, les assureurs essaient de mettre en place des nouveaux produits d'assurance"[266].

Le 11 novembre 2019, la *Lloyds Market Association* décide d'adopter la clause LMA 5403, dans le but d'essayer de clarifier l'interprétation de l'exclusion 380.

Toutefois, bien qu'il s'agit clairement d'une avancée partielle vers la précision de la limite de l'exclusion, cette nouvelle clause risque d'apporter des confusions supplémentaires[267].

Dans son premier paragraphe la clause stipule : *"1. Sous réserve du seul paragraphe 3 ci-dessous, cette assurance ne couvre en aucun cas les*

[262] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.,* p.2.
[263] *Cf.,* WTW, HILL A., *"Silent Cyber: ce que vous devez savoir"*, 07 juin 2021, https://www.wtwco.com/fr-ch / insights/2021/01/silent-cyber-what-you-need-to-know, Consulté le 12/08/2023.
[264] Astaara Co. Limited, *"LMA 5403, a lost opportunity ?"*, *op.cit.,* p.3.
[265] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.* p.2.
[266] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , *op.cit.*, p. 3.
[267] Astaara Co. Limited, *"LMA 5403, a lost opportunity ?"*, *op.cit.*, p.3.

pertes, dommages, responsabilités ou dépenses directement ou indirectement causés par l'utilisation ou l'exploitation, d'un ordinateur ou d'un système informatique, ou découlant de l'utilisation ou de l'exploitation, comme moyen d'infliger un préjudice[268]*, d'un programme informatique, code malveillant, virus informatique, processus informatique ou tout autre système électronique"*[269].

A première vue, nous pouvons considérer comme garanti, le sinistre lié à un risque cyber dont le fait générateur n'était pas utilisé ou exploité *"comme moyen d'infliger un préjudice"* ou tel que les termes anglais l'exprime *"as a means for inflicting harm"*. Toutefois, des questions perdurent[270].

D'abord, quelle est la définition du terme *"harm"* ?

Ce mot peut signifier différentes choses pour différentes personnes. A titre d'exemple, le dictionnaire anglais identifie *harm,* comme une blessure ou un dommage matériel physique[271]. La loi britannique sur l'usage abusif des ordinateurs de 1990[272], se réfère à l'utilisation non autorisée des ordinateurs causant des dommages soient matériels directs, soient portant préjudice à la santé humaine, l'environnement, l'économie ou la sécurité nationale. Dans d'autres législations, ce terme est assimilé aux blessures et préjudices physiques.[273]

En conséquence, "*le flou entourant la définition de cette notion clef va continuer à entraîner des interprétations difficilement anticipables lors de la souscription du risque. Le « silent cyber cover » que les assureurs comme les assurés souhaitent voir disparaître devrait perdurer "*[274].

---

[268] Souligné par nous même.
[269] Marine Cyber Exclusion endorsement Clause (LMA5402), Lloyd's Market Association, november 11th 2019 ,https://www. lmalloyds.com/LMA/News/ LMA_bulletins/LMA_Bulletins/LMA19-031 PD.aspx., *"1. Subject only to paragraph 3 below, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly 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, computer process or any other electronic system…".*
[270] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.* p.2.
[271] Cambridge dictionary, *"harm, means physical or other injury or damage".*
[272] The Computer Misuse Act of 1990, *Cf.,* https://www.legislation.gov.uk/ukpga/1990/18/contents.
[273] Astaara Co. Limited, *"LMA 5403, a lost opportunity ?"*, *op.cit.* p.3.
[274] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.* p.2.

De ce fait, la clause LMA 5403, comme l'a fait la clause LMA 5402[275] va exclure la couverture des dommages résultant des actes cyber malveillants. *A contrario,* une police contenant une clause LMA 5403 pourrait assurer des actes cyber *"non malicious"*.

Le paragraphe 3 de la clause LMA 5403, similaire à celui de la CL 380, lève l'exclusion s'agissant des dommages résultant des attaques cyber en rapport avec les actes de guerre, dans le cas où le navire assuré est déjà garanti par une police ou clause couvrant le risque de guerre.

Ensuite, comme c'était le cas avec la clause 380, la LMA 5403 est également silencieuse quant au rôle du *"Head Office"* de l'armateur, en tant que vecteur important dans le contrôle et la gestion de l'attaque cyber[276].

Selon ces clauses, nous n'avons pas d'informations claires si le *"Head Office"* de l'armateur est considéré comme victime, ou s'il participe à l'attaque de l'extérieur ou bien s'il est la source même de l'attaque[277].

Pour finir, la problématique concernant le caractère intentionnel de l'attaque reste encore non résolue. Avec la formulation : *"As a means of inflicting harm",* on a du mal ici aussi à désigner le coupable et à vérifier si l'acte est intentionnel ou pas.

Par ailleurs, "*La LMA 5403 ramène le marché de l'assurance aux interrogations de la clause 380 concernant l'intentionnalité et le caractère proche (« proxima ») ou distant (« remote ») de la cause"*[278].

Pour conclure, il est essentiel de noter que l'introduction de ces clauses dans les polices maritimes, d'emblée, ne devait servir que de guide et d'inspiration pour les assureurs et non de règle générale. Nicholas Gooding déplore d'ailleurs l'utilisation systématique et généralisée de la clause CL 380

---

[275] The Marine Cyber Exclusion Clause (LMA5402) states: *"This clause shall be paramount and shall override anything in this insurance inconsistent therewith. 1 In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from: 1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or 1.2 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 other electronic system"*.

[276] Astaara Co. Limited, *"LMA 5403, a lost opportunity ?"*, *op.cit.* p.3.

[277] *Ibid.*

[278] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, *op.cit.* p.2.

et la LMA 5403. Il est d'avis que ces dispositions : " …*devraient être utilisées de façon appropriées et applicables au risque en question [et constituent] des clauses de protection contre une accumulation inacceptable de risques découlant d'une cyberattaque*"[279].

L'usage aveugle de ces clauses d'exclusion est perçu comme un obstacle à la protection contre les risques cyber auxquels est confronté le secteur maritime, ce qui pousse davantage l'industrie à l'introduction de nouveaux produits assurantiels et à l'examen de la pertinence de ces clauses d'exclusion cyber.

La non couverture de la menace *"marétique"* peut aussi être expliquée par son assimilation à des risques déjà exclus des polices maritimes ordinaires (2).

2. La menace cyber maritime, un risque lié à des exclusions générales :

L'exclusion de la couverture du risque *marétique* peut aussi découler de son association à des risques préalablement exclus des polices maritimes ordinaires, tel que notamment le risque de guerre ou de piraterie…

Cette menace assez nouvelle et atypique peut venir en concours avec d'autres catégories de risques comme les risques de guerre[280]. Dans un cas pareil, l'éventualité que ce risque soit soustrait de la garantie d'assurance reste valable, notamment s'il est question d'une police d'assurance qui assure les cyber risques mais ne couvre pas les risques de guerre.

Bon nombre des cyberattaques, les plus sophistiquées proviennent d'États-nations ou de cybercriminels subventionnés par des États belligérants ;

---

[279] BREWER J., "*Marine Insurance Market is Sharpening its Focus on Cyber Attack Risk."*, ALL ABOUT SHIPPING.Co.UK, May 25, 2015, www.allaboutshipping.co.uk/2015/05/25/ marine-insurance -market-is-sharpening -its-focus-on-cyber-attack-risk/, (145)., in. KAO M.-B., *"Cybersecurity in the Shipping Industry and English Marine Insurance Law"*, Tulane Maritime Law Journal, vol. 45, no. 3, summer 2021, p.488. Traduit par nous même.

[280] EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"* Adam Assurances, Le Lab, 22 octobre 2019, https://f.hypotheses.org/wp-content/blogs.dir/4944/files /2019/10/T % C3%A9l%C3%A9charger-4.pdf, p.1, Consulté le 12/08/2023.

la question de savoir si ces attaques cyber sont considérées comme des "actes de guerre" est actuellement controversée[281].

Plusieurs affaires sont d'ailleurs en cours de traitement devant les tribunaux du monde entier, dans le but de clarifier, ce qui constitue clairement un acte de guerre, et donc à déterminer si les cyberattaques, dont les auteurs sont des États, sont couvertes ou pas[282].

De ce fait, *"si le risque cyber peut coexister avec d'autres catégories de risques à l'instar des risques de guerre, un assureur qui offre une couverture pour cette dernière catégorie de risques peut-il être appelé à indemniser son client des conséquences d'une attaque cyber ? Ou inversement, un assureur cyber peut-il invoquer l'existence d'un risque de guerre dans le contexte d'une attaque cyber pour rejeter toute demande d'indemnisation de son client ?"* [283].

A ce niveau, les difficultés relatives à la frontière qui sépare le risque cyber des risques de guerre, sont bien visibles[284]. L'affaire *Mondelez International, Inc. c/ Zurich American Insurance company*[285] relative à l'indemnisation des conséquences de l'attaque cyber NotPetya, pendante devant une Cour suprême américaine, illustre clairement cette ambivalence.

Cette affaire paraît particulièrement pertinente étant donné qu'il s'agit de "*...la première fois qu'une compagnie d'assurance se prévaut de l'exclusion des risques de guerre pour contester la couverture d'une attaque cyber. L'issue de cette affaire pourrait avoir d'importants impacts sur le contenu et les limites des futurs contrats d'assurance cyber"*[286].

Dans ce sens, il serait intéressant de voir comment va se tracer le mapping de la *"cyberguerre"* et comment il serait associé aux périls de guerre,

---

[281] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ",* Thetius, Cyberowl, et HFW, 2022, p.33. Traduit par nous même.
[282] *Ibid.*
[283] EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"*, *op.cit.*
[284] *Ibid*.
[285] *Cf.* GREENWALD J.*, " Silent cyber ruling has insurers looking closer at war clause",* Business Insurance, Risk Management, March 04th, 2022, https://www.businessinsurance.com/article/20220304/NEWS06/912348162 /Silent-cyber-ruling-has-insurers-looking-closer-at-war-clause, Consulté le 12/08/2023.
[286] EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"*, *op.cit.*

tant en matière de développement de produits d'assurance que d'intervention judiciaire[287].

En principe, les cyber attaques n'impliquent pas un recours aux armes ni à la force. Ceci peut être une piste pour essayer de séparer les deux risques. Toutefois, cette distinction, dans certaines circonstances, peut se révéler insensée, surtout quand l'origine et l'intérêt de l'attaque sont inconnus [288].

Concrètement, pour être qualifié comme acte de guerre, une attaque doit engendrer des blessures et des dommages physiques et éventuellement des pertes humaines. Si on suit ces critères, il y a moyen, éventuellement de qualifier les cyberattaques, qui engendrent indirectement des dommages matériels physiques, comme actes de guerre. C'est le cas notamment du virus informatique Stuxnet qui avait pénétré les systèmes de centrifugeuses en Iran, entraînant des accidents graves et des pertes en vies humaines[289].

En pratique, avec les conventions spéciales, la garantie Waterborne et la garantie Etendue, qui couvrent le risque de guerre maritime en corps et en facultés, on ne trouve aucune mention, pour couvrir aussi les dommages liés aux attaques cybernétiques[290].

"Cependant, dans la mesure où le risque de guerre peut prendre la forme d'un risque cyber, l'application de la clause d'exclusion cyber CL 380

---

[287] JACKSON S., *"Cyber 'war': a question of 'reasonable expectations",* Clyde&Co, IUMI EYE Newsletter, Mars 2022, n°36, p.11.

[288] EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"*, *op.cit*., p.3.

[289] N. SCHMITT M., Tallinn Manual 2.0 on the International Law applicable to cyber operations, *éd.*, Cambridge University Press, 2017, Règle 14, p. 84, note (4), *in.,* EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"*, *op.cit*., p.3.

[290] Conventions spéciales RG WB 2018 pour l'assurance des facultés (marchandises) transportées par voie maritime contre les risques de guerre, de terrorisme et de grève, Garantie Waterborne du 1er juillet 2018, ARTICLE 2 : *"- Risques couverts 1°) Les présentes Conventions Spéciales ont pour objet de garantir les marchandises assurées contre les dommages et pertes matériels, ainsi que les pertes de poids ou de quantités résultant de : a) guerre civile ou étrangère, hostilités, représailles, émeutes, mouvements populaires ; b) explosion de torpilles, mines et tous autres engins de guerre autres que ceux destinés à exploser par modification de structure du noyau de l'atome et, généralement, de tous accidents et fortunes de guerre ; c) actes de sabotage et/ou de terrorisme qui ont un caractère politique ou qui se rattachent à la guerre ; d) captures, prises, arrêts, saisies, contraintes, molestation ou détention par toutes autorités gouvernementales quelconques ; e) grèves, lockout et autres faits analogues ; f) piraterie ayant un caractère politique ou se rattachant à la guerre…".*

[dans la police ordinaire] serait-elle suffisante pour contester des réclamations fondées sur un événement cyber caractéristique d'un risque de guerre ?" [291].

La frontière entre le risque cyber et le risque de guerre apparaît alors très ténue [292].

Enfin, il convient de noter que la séparation des périls de guerre des périls de mer, et donc la nécessité de les catégoriser, est un domaine en développement depuis des centaines d'années[293]. Ce qu'on appelle aujourd'hui la *"Cyberguerre"* constitue désormais une guerre moderne plus décentralisée et asymétrique, qui soulève ses propres défis, notamment quant à sa couverture en assurance[294].

Le risque cyber dans le monde maritime est aussi souvent lié à la piraterie.

L'article 101 de la Convention des Nations unies sur le droit de la mer[295] définit la piraterie maritime comme *"un acte illicite de violence ou de détention ou de déprédation commise par l'équipage ou des passagers d'un navire (...) agissant à des fins privées (...) en haute mer*".

Échappant de toute autorité étatique en Haute mer, le pirate bénéficie d'une grande liberté pour circuler dans le milieu maritime.

A cet effet,*"la souplesse de l'instrument donne une prime au maître de la mer, libre d'attaquer à de multiples endroits"* [296]. Dans ce sens, il suffit de remplacer "maritime" par "numérique" et substituer le groupe des pirates par des cybercriminels[297], et la scène d'une cyberattaque maritime serait complète.

---

[291] EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"*, *op.cit*., p.3.
[292] *Ibid.,* p.4.
[293] JACKSON S., *"Cyber 'war': a question of 'reasonable expectations", op.cit.,* p.11.
[294] *Ibid.*
[295] Article 101 de la Convention des Nations unies sur le droit de la mer (CMB), il "*...exige, en effet, actuellement que l'acte se soit déroulé en haute mer, excluant par conséquent les actes commis dans les eaux territoriales ou intérieures d'un État, lesquels relèvent dès lors de la seule juridiction territoriale de cet État côtier". Cf.* BELLAYER-ROILLE A., *"Entre souveraineté et transnationalité, les défis du droit de la mer",*Revue internationale et stratégique, 2014/3, n° 95.
[296] COUTEAU B., 1995, *in*. MANET F-C.., *"La marétique, un enjeu essentiel pour l'humanité ?", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p. 83.
[297] MANET F.-C, *"La marétique, un enjeu essentiel pour l'humanité ?", op.cit.,* p.83.

Concernant la piraterie, *"le marché français opère pour leur couverture, une distinction entre la piraterie dite lucrative et la piraterie à caractère politique se rapportant à la guerre"*[298].

La piraterie lucrative est couverte par la police risques ordinaires et la piraterie à caractère politique ou se rapportant à la guerre, exclue selon l'article 7 de la police française d'assurance maritime sur facultés, est prise en charge par la police spéciale, prévue contre les risques de guerre[299].

Jusqu'à présent, les pirates restent actifs malgré les mesures dissuasives prises par les acteurs maritimes. Leur aptitude à s'adapter et à changer constamment leurs stratégies d'attaques, leur permettent de relever les défis posés par les mesures de prévention et de protection adoptées[300].

A ce niveau, il semble judicieux de mettre en évidence que *"...si les initiatives visant à contrer la cyber-menace en général se multiplient ces derniers temps, y compris dans l'industrie maritime, cette dernière semble encore peu encline à prendre au sérieux la possible collusion entre piraterie et cyber-risque"*[301].

En réalité, de nombreux incidents démontrent une interdépendance des deux menaces, d'autant plus évidente avec le développement des nouvelles technologies numériques, dans le secteur du commerce maritime.

En témoigne l'enquête menée par Verizon, pour le compte d'un grand armateur, ayant subi de multiples attaques sur ses navires[302]. L'étude de cas, connue sous le nom de *"Roman Holiday"* illustre une série d'attaques, dans lesquelles les pirates étaient au courant d'informations très spécifiques concernant la cargaison à bord des navires. Les pirates montaient à bord, forçaient l'équipage dans une seule zone, puis partaient très rapidement après avoir volé les cargaisons dont ils connaissaient à l'avance leur localisation[303].

---

[298] EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"*, *op.cit*., p.3.
[299] *Ibid.*, pp.3-4.
[300] BENOTTI S., "*Piraterie maritime : la maîtrise du risque ?"*, ISEMAR, Note de synthèse, n° 199, avril 2018, p. 3-4.
[301] *Ibid.,* p.4.
[302] VERIZON, *"Data breach digest report : Scenarios from the field"*, 2016, p.55, https://maritimecyprus. com/ wp- content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf, Consulté le 13/08/2023.
[303] Seatrade Maritime News, *"Cyber-attack allows pirates to target cargo to steal",* 07 juillet 2016, https:// www. seatrade - maritime. com/ americas /cyber-attack-allows-pirates-target-cargo-steal, Consulté le 13/08/2023.

Évidemment, la piraterie n'est pas un nouveau problème pour cette (ou toute autre) compagnie maritime. Cependant, dans ces derniers mois, la victime avait remarqué un changement de tactique de la part des pirates, d'une manière qu'elle a trouvé extrêmement déconcertante[304]. Plutôt que de passer des jours à tenir les bateaux et leur équipage en otage, pendant qu'ils fouillent dans la cargaison, ces pirates ont commencé à attaquer les navires d'une manière extrêmement ciblée et rapide [305].

Finalement, les soupçons sont tombés sur le système de gestion de contenu (CMS) de l'entreprise à travers lequel les connaissements sont téléchargés. En étudiant le trafic réseau autour du CMS, Verizon a découvert qu'un *shell web* malveillant avait été téléchargé sur le serveur, ce qui a permis aux pirates d'interagir avec le serveur Web et d'effectuer des actions telles que le téléchargement de données, notamment des connaissements pour les futures expéditions[306].

A travers cet exemple, nous pouvons, dès lors, comprendre la démarche que certains pirates suivent pour mieux cibler les bâtiments à attaquer en évaluant en amont leur vulnérabilité et les bénéfices pouvant résulter d'une attaque réussie[307].

Actuellement, la scène maritime semble sceptique quant à l'association des risques cyber aux risques de piraterie. "*En témoignent les Guidelines on cyber security on board ships*[308] *publiées par les associations professionnelles ces deux dernières années et dans lesquelles le terme de « piraterie » n'apparaît qu'une fois au sein d'un document d'une cinquantaine de pages…*"[309].

Il va sans dire que les deux menaces ne sont pas identiques de part leur nature et leur étendue, or l'éventualité de la rencontre de ces risques reste envisageable.

---

[304] VERIZON, *"Data breach digest report : Scenarios from the field"*, *op.cit.,* p.55.
[305] *Ibid.*
[306] Seatrade Maritime News, *" Cyber-attack allows pirates to target cargo to steal", op.cit.*
[307] BENOTTI S.,"*Piraterie maritime : la maîtrise du risque ?"*, *op.cit.*, p. 3.
[308] *Cf.,* BIMCO, The Guidelines on cyber security on board ships, version 4, 2020, Downloads/ Guidelines% 20on%20Cyber%20Security%20Onboard%20Ships%20V4%20(1).pdf, Consulté le 13/08/2023.
[309] BENOTTI S., "*Piraterie maritime : la maîtrise du risque ?"*, *op.cit.*, p. 4.

Avec le temps, la piraterie continue d'évoluer et les méthodes auxquelles les pirates ont recours deviennent de plus en plus automatisés et sophistiqués. La piraterie *"...prend un nouveau tournant, avec nos sociétés, administrations et entreprises qui dépendent toujours plus de l'outil informatique et des réseaux de communication"*[310].

Concernant le volet assurantiel, l'exclusion de la couverture en assurance d'un acte de piraterie lucrative, basé sur une cyber menace , est selon nous, l'hypothèse la plus probable et logique. " *...Conformément aux critères de qualification proposés par la doctrine, un événement cyber peut avoir les caractères d'un acte ou fait de guerre dès que les équipements électroniques de communication et de navigation subissent un quelconque dommage du fait de l'attaque cyber*" [311].

De ce fait, la piraterie lucrative, comme son homologue la piraterie politique, une fois fondée sur une attaque cyber et causant un dommage matériel, quel qu'il soit, elle serait automatiquement assimilée à un risque de guerre. Ce qui impliquerait éventuellement une exclusion de couverture sous les polices ordinaires, des risques de piraterie, de toute sorte, politique ou lucrative, si elle est liée à une menace cyber[312]. A cet égard, la distinction entre piraterie lucrative et politique n'aurait plus d'intérêt pratique[313].

A ce niveau, il nous semble impératif, pour les opérateurs maritimes, de dresser clairement les frontières entre ces différents risques entremêlés : guerre, piraterie et menace cybernétique, capables d'engendrer des confusions et des exclusions assurantielles abusives.

Un long chemin reste à parcourir afin d'assurer une protection exhaustive face à ces éventuelles menaces.

"Les difficultés à mettre en place une telle garantie sont ...nombreuses, quant aux risques précisément couverts, quant aux causes d'exclusion (notamment au regard de l'attitude de l'entreprise victime et de ses

---

[310] KERMARREC Y., *" Cybersécurité et monde maritime : contexte, enjeux, challenges et opportunités",* DMF, nº 842, 1er janvier 2022, p.2.
[311] EDORH-KOMAHE P.-A., *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"*, *op.cit*., p.5.
[312] *Ibid.*
[313] *Ibid.*

salariés), ou encore quant aux frais et dommages compris dans la couverture d'assurance"[314].

Mais, des lueurs d'espoir commencent, déjà, à se manifester laissant entrevoir une progression tangible vers la couverture du risque cyber dans le domaine du transport maritime (B).

[314] PIETTE G., Traité du Droit maritime, 2023, *op.cit.*, p.543.

B)- Une évolution visible vers la garantie du risque cyber en transport maritime

Tel que rappelé par Jean BAYON DE LATOUR, directeur gérant du Cyber Head à MARSH (courtier d'assurance maritime), lors du PARISMAT 2023, dans le cadre d'une table ronde sur la réaction de l'écosystème maritime face au risque cyber [315], il existe bel et bien une demande de plus en plus grandissante pour les assurances cyber en transport maritime, comme il existe également une offre qui se développe au fil du temps.

Lors de cette conférence, Howard POTTER, membre du comité de la prévention des dommages au IUMI, explique également, le retard de la mise en place d'une assurance cyber maritime et la réticence des assureurs quant à ce sujet, par le décalage dans le temps, entre l'existence du monde maritime, qui date de plusieurs centaines d'années et celui du cyber risque, qui ne remonte qu'à une vingtaine d'années[316]. Ainsi, pour ajuster le cyber au maritime, il faut passer par tout un processus d'apprentissage essentiel, afin d'arriver au niveau de maturité recherché.

Personne ne peut, donc, nier le retard que l'industrie maritime a pris, par rapport aux autres industries, dans l'intégration du risque cyber à ses principales préoccupations. Divers autres secteurs, notamment le secteur de la défense et le secteur bancaire[317], ont certainement pris de l'avance, en investissant sans tarder dans la cybersécurité, chose qui leur a permis une meilleure sécurité et protection face aux cyberattaques.

Actuellement, les efforts fournis par le marché assurantiel maritime visant une couverture des risques cybernétiques, sont en plein développement.

[315] CESAM, PARISMAT 2023, table ronde : Comment l'écosystème maritime et aérien fait face à la montée du risque cyber ? , 27 juin 2023, intervention disponible sur : https://www.youtube.com/watch?v=vIEMAeHusno, Consulté le 14/08/2023.
[316] *Ibid.*
[317] *Ibid.*

A cet effet, le marché d'assurance britannique était le premier à se démarquer en proposant des solutions permettant de préserver un degré de cybersécurité maritime, capable de faire face aux éventuelles cyberattaques.

"En février 2016, le BIMCO[318] *et d'autres organisations (parmi lesquelles Intertanko,…IUMI) ont publié des "Guidelines on cyber-security onboard ships", dont l'objectif est d'identifier les menaces et les vulnérabilités, et de développer des mesures de protection"*[319]. Ces guides ont été constamment révisés pour pouvoir s'adapter au rythme évolutif et changeant des cyber risques.

En 2019, la volonté proactive du marché britannique, d'adapter les produits d'assurance pour répondre à ces défis cybernétiques, était également mise en évidence à travers la création par le BIMCO d'une clause-type traitant des questions de cybersécurité : la *Cyber Security Clause*[320].

Cette clause se divise en quatre sections. Les deux premières invitent les parties concernées à garantir leur propre cybersécurité et à s'assurer que les tiers qui fournissent des services pour leur compte suivent également cette voie. Elles englobent la mise en œuvre des mesures et des moyens de cybersécurité adéquats, le maintien constant de leur niveau de cybersécurité, l'établissement de procédures appropriées pour réagir aux incidents, ainsi qu'une incitation à la révision périodique de leurs stratégies en matière de cybersécurité[321]…

La troisième section exige qu'une des parties informe promptement son cocontractant de tout incident relatif à la cybersécurité qui impacte ou pourrait impacter la sécurité informatique de l'une des parties[322].

---

[318] BIMCO, The Guidelines on cyber security on board ships, version 4, 2020, Downloads/ Guidelines% 20on%20Cyber%20Security%20Onboard%20Ships%20V4%20(1).pdf, Consulté le 13/08/2023.
[319] PIETTE G, *" Le commerce maritime face au risque cyber"*, *op.cit.* , p.2.
[320] BIMCO, Cyber Security Clause 2019 : " *(a) Each Party shall:*
(i) implement appropriate Cyber Security measures and systems and otherwise use reasonable endeavours to maintain its Cyber Security;
(ii) have in place appropriate plans and procedures to allow it to respond efficiently and effectively to a Cyber Security Incident; and
(iii) regularly review its Cyber Security arrangements to verify its application in practice and maintain and keep records evidencing the same…", https://www.bimco.org/contracts-and-clauses/bimco- clauses /current/ cyber-security-clause-2019, Consulté le 13/08/2023.
[321] PIETTE G, *" Le commerce maritime face au risque cyber"*, *op.cit.* , p.2.
[322] *Ibid.*

Enfin, la quatrième section prévoit une clause de limitation de responsabilité en faveur de la partie qui ne s'est pas conformée aux obligations découlant de cette clause. "*A défaut de stipulation contraire, le montant de cette limitation est de 100.000 US Dollars. Cette limitation est exclue s'il est démontré que la partie en question a commis une négligence grave ou une faute intentionnelle"*[323].

Diverses interrogations surgissent, donc, concernant les responsabilités qui incombent à l'assuré ainsi que la portée de la couverture d'assurance.

Actuellement, les différentes polices d'assurance disponibles proposent de garantir le rachat des clauses d'exclusion visant spécifiquement les navires[324]. Certes, cette possibilité de racheter les clauses d'exclusion des risques cyber des polices maritimes corps (CL 380 et LMA 5403) est désormais envisageable. En revanche, la garantie du risque ne pourrait être automatique. Il existe indubitablement des conditions qui doivent être respectées, afin de faire courir l'assurance.

A ce titre, *"la croissance de la menace et la non-maturité des marchés de l'assurance obligent les entreprises à accroître leur niveau de prévention du risque cyber afin d'une part de s'en prémunir et d'autre part d'optimiser leurs chances d'accéder à une garantie d'assurance adaptée"*[325].

Dès lors, on invite les armateurs, à prendre les mesures de prévention et de cyber résilience nécessaires, afin d'éviter au maximum le risque cyber, mais également pour profiter de la couverture de l'assurance cyber.

Dans ce contexte, plusieurs assureurs, afin d'échapper à la garantie d'un risque cybernétique maritime, plaident souvent l'innavigabilité du navire.

Il est essentiel, d'abord, de rappeler que l'obligation de mise à disposition d'un navire en bon état de navigabilité est une obligation de résultat, qui incombe à l'armateur[326]. Le Marine Insurance Act de 1906 considère qu'un

[323] PIETTE G, *" Le commerce maritime face au risque cyber"*, *op.cit.* , p.2.
[324] PERRA F., *" Les principes de l'assurance du risque cyber pour les compagnies maritimes"*, DMF n°842, 01 janvier 2022, p.4.
[325] *Ibid*.
[326] PIETTE G, *" Le commerce maritime face au risque cyber"*, *op.cit.* , p.2.

navire est en bon état de navigabilité, s'il est capable de faire face *"aux dangers ordinaires"* au cours du voyage assuré[327]. Par conséquent, les armateurs sont tenus de rendre le navire en bon état de navigabilité et non simplement de faire de leur mieux pour le réaliser.

Selon l'affaire *McFadden v. Blue Star Line*[328], un cas portant sur la navigabilité dans un contrat de transport plutôt qu'en assurance maritime, un navire est considéré en bon état de navigabilité, s'il possède *"le conditionnement physique qu'un propriétaire ordinaire, attentif et prudent exigerait de son navire au début de son voyage, en tenant compte de toutes les circonstances probables qui l'entourent"*[329].

En résumé, un bon état de navigabilité comprendrait trois aspects : l'état physique du navire et de l'équipement à bord, la formation et le nombre d'équipages, et la documentation appropriée, permettant le navire de faire le voyage nécessaire[330].

De son côté, la jurisprudence américaine évoque un autre concept semblable à cette condition. Il s'agit de *"pratiques de sécurité minimum"*ou *(Minimum Required Practices),* auxquelles l'assuré doit recourir afin de limiter le dommage et d'assurer la menace cybernétique. L'assureur en l'espèce avait engagé une action devant un Tribunal fédéral à Los Angeles, en soutenant qu'il n'était pas obligé de couvrir le risque, au motif que l'assuré n'avait pas recouru à des *« pratiques de sécurité minimum »*[331]. L'assuré devait régulièrement maintenir des mécanismes de gestion de sécurité sur son système, et en ne le faisant pas, il s'est exposé au risque en question[332].

---

[327] Marine Ins. Act, 1906, 6 Edw. 7, ch. 41, § 39(4) (Eng.), note (162), *in.,* KAO M.-B., *"Cybersecurity in the Shipping Industry and English Marine Insurance Law"*, *op.cit.,* p.492. Traduit par nous même.

[328] En l'occurrence, le plan de passage défectueux a rendu le navire innavigable parce que, à la suite d'un test juridique établi de longue date, *un propriétaire prudent* aurait exigé que le plan de passage soit rectifié avant le début du voyage. L'affaire a aussi posé l'obligation de faire preuve de diligence raisonnable pour rendre un navire en état de navigabilité avant et au début du voyage. Il s'agit d'une obligation personnelle et non transmissible pour le propriétaire, peu importe qui le propriétaire avait chargé pour accomplir cette tâche, *Cf.* MARITIME MUTUAL, *"Defective passage plans and unseaworthiness : english supreme court decision in the CMA CGM Libra grounding case",* Maritime Mutual Risk Bulletin No. 53, 11 January, 2022, https://maritime-mutual. com/risk-bulletins/defective-passage- plans-and-unseaworthiness-english-supreme- court-decision- in -the-cma-cgm-libra-grounding-case, Consulté le 13/08/2023. Traduit par nous même.

[329] KAO M.-B., *"Cybersecurity in the Shipping Industry and English Marine Insurance Law"*, *op.cit.,* p.492. Traduit par nous même.

[330] *Ibid.*

[331] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , *op.cit.*, p.4.

[332] *Ibid.*

De facto, pour pouvoir bénéficier de la couverture d'assurance cyber maritime, il faut faire le nécessaire afin de garantir le bon état de navigabilité de son bâtiment, ou encore mettre en œuvre les pratiques de sécurité minimales, pour éviter dès le début, le déroulement de l'incident ou encore limiter l'impact du dommage, si l'incident se produit.

A cet égard, il semble être opportun de rappeler également que le rachat des clauses d'exclusion du risque cyber, incorporées dans les polices maritimes, ne couvre que les risques matériels physiques. Tous les potentiels dégâts non matériels qui peuvent résulter d'un cyber incident ne seront pas garantis. On cite notamment, les frais de remise en marche des systèmes informatiques, les frais liés au retard, les frais de remplacement du matériel qui n'est pas visé directement par la cyberattaque, les coûts de perte d'exploitation, etc[333].

Pour combler ce vide, les courtiers d'assurances, tel que MARSH, proposent aux clients, souhaitant garantir également les risques immatériels, de souscrire à des polices cyber non maritimes, indépendantes de la police maritime ordinaire pour corps ou facultés[334].

Nonobstant le fait que le risque cyber immatériel peut être couvert par une garantie silencieuse, de nombreux armateurs et chargeurs, choisissent, aujourd'hui, d'adhérer à des polices d'assurance cyber, mise à part des polices maritimes, afin d'éviter l'incertitude de ces couvertures silencieuses.

Ce type de police vise généralement, "*...la couverture des atteintes au système d'Information de l'assuré telles que : tout dysfonctionnement, altération, perturbation ou indisponibilité de tout ou partie du système d'information de l'assuré ainsi que toute atteinte à l'intégrité, la confidentialité, ou la disponibilité des données"*[335].

---

[333] CESAM, PARISMAT 2023, table ronde : *Comment l'écosystème maritime et aérien fait face à la montée du risque cyber ?*, *op.cit.*
[334] *Ibid.*
[335] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , *op.cit.,* p.3.

En somme, ces polices couvrent les atteintes au système d'information de l'assuré, y compris, la possibilité d'accéder, donner, supprimer ou restreindre l'accès de manière non autorisée, dans tout ou partie du système d'information de l'assuré[336]. Les frais d'investigation numérique, de consultants désignés afin de connaître la source de l'incident, entrent également dans le périmètre[337]. Les garanties souscrites peuvent aussi englober les coûts additionnels d'exploitation et l'indemnisation des pertes d'exploitation[338].

Pour ce qui est de la légalité des paiements de rançons, ce sujet reste encore controversé. Le paiement de rançon ne devrait être qu'une question de dernier recours lorsque la sécurité est compromise. Même dans ces circonstances, la légalité du paiement peut être difficile à évaluer en temps réel. Cela est vrai pour les victimes de l'attaque, et pour chaque entité et individu impliqués dans la facilitation du paiement, y compris les assureurs[339].

"A ce jour il n'existe pas d'interdiction légale ou réglementaire expresse d'assurer ce risque. Toutefois plusieurs réserves réglementaires, morales et financières…"[340] subsistent.

Comme nous avons pu le voir, les marchés d'assurance maritime et de la cyber assurance offrent, depuis un certain moment, divers produits pour couvrir l'exposition des armateurs aux cyberrisques. Alors que la majorité des produits de cyber assurance maritime se concentrent sur la couverture d'interruption d'activité, une simple minorité couvrira les dommages physiques aux navires et aux marchandises[341]. Ceci s'explique essentiellement par la probabilité qu'un incident cyber entraîne des dommages physiques matériels et non pas par l'indisponibilité de l'offre sur le marché assurantiel.

---

[336] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , *op.cit.,* p.3.
[337] *Ibid.*
[338] *Ibid.,* p.4.
[339] CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry ",* Thetius, Cyberowl, et HFW, 2022, p.39. Traduit par nous même.
[340] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , *op.cit.,* p.4.
[341] HOLMAN FENWICK WILLAN, *"Cyber risk adaptability and responsibility"*, December 2020, p.3. Traduit par nous même.

Les couvertures P&I, quant à elles, doivent déjà répondre aux cyberincidents, à l'exception des exclusions habituelles relatives aux risques de guerre et au terrorisme[342].

"*D'une manière générale, et contrairement à la plupart des autres formes d'assurance maritime, les règles (ou conditions de base de couverture) des P&I clubs, n'excluent pas les réclamations résultant d'incidents cybernétiques, sauf si un tel incident était considéré comme un acte de guerre ou de terrorisme"*[343].

Par conséquent, la protection ordinaire du P&I serait accessible pour les résultats d'un incident cyber lié à des événements autres que des actes de guerre ou de terrorisme. Ces circonstances pourraient inclure, à titre d'exemple, des simples problèmes survenant à l'ordinateur à bord, des défaillances causées involontairement par des manipulations à distance des systèmes embarqués, ou même des actes de destruction intentionnelle perpétrés par des anciens employés mécontents[344].

Cependant certains cas restent exclus. *"Les risques « cyber or not » qui ne trouvent pas leur origine dans une opération liée au navire sont exclus"*[345]. A titre d'exemple, le risque financier lié au paiement d'une rançon afin de restaurer le SI d'une compagnie maritime, suite à une attaque par rançongiciel, n'est pas inclus[346].

Dans le but de clarifier la situation, plusieurs P&I clubs, dont *"The American Bureau of Shipping",* mettent en place une liste de règles à respecter afin de pouvoir bénéficier de la protection P&I.

Bien qu'il n'y ait pas d'exclusion explicite en matière de cybersécurité dans les règles de *l'American Club,* les membres doivent agir avec prudence et prendre toutes les mesures raisonnables afin d'éviter ou de minimiser toute dépense ou responsabilité qui pourrait découler des cyberrisques[347]. De ce fait,

---

[342] HOLMAN FENWICK WILLAN, *"Cyber risk adaptability and responsibility"*, *op.cit.,* p.3.
[343] THE AMERICAN CLUB, ABS GROUP, *"Managing cyber risks and the role of the P&I club : an overview",* october 2020, p.2. Traduit par nous même.
[344] *Ibid.*
[345] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , *op.cit.,* p.3.
[346] *Ibid.*
[347] THE AMERICAN CLUB, ABS GROUP, *"Managing cyber risks and the role of the P&I club : an overview", op.cit.*, p.2.

les membres devraient adopter une cyber résilience appropriée, sinon la couverture du P&I pourrait être compromise[348].

Nous trouvons également certaines *"Rules"* des P&I Clubs qui ne couvrent pas les sinistres dont l'origine provient de l'utilisation d'un *"trading system"* n'ayant pas été approuvé par le Club[349].

Enfin, comme nous avons pu le voir avec les assurances maritimes et non maritimes du cyber risque, la couverture P&I, elle aussi, est soumise à des conditions et des règles spécifiques pour la faire activer, en particulier l'état de navigabilité du navire avant le voyage et son niveau de préparation face à une potentielle cyberattaque.

Sur cette question, les assureurs travaillent en étroite collaboration avec les sociétés de classification dans le but d'améliorer la sécurité du transport maritime.

Dans cette optique, en 2015, l'association internationale des sociétés de classification (IACS)[350] a introduit un cyber panel et a formé un *« Groupe de travail conjoint sur les cyber systèmes »* avec l'industrie IUMI[351]. "*Cette initiative a été créée pour améliorer la capacité de l'Association à répondre aux préoccupations en matière de cybersécurité tout en appuyant la protection de la vie humaine, des biens et du milieu marin"*[352].

A cet égard, les sociétés de classification ont développé des notations spécifiques à la cybersécurité. Le Bureau Veritas, par exemple, a élaboré deux classements spécifiques (SW Registry et SYSCOM) relatifs aux logiciels utilisés dans les systèmes embarqués et la cybersécurité dans l'échange de données entre le navire et la terre[353].

---

[348] THE AMERICAN CLUB, ABS GROUP, *"Managing cyber risks and the role of the P&I club : an overview", op.cit.*, p.2.
[349] PERRA F., *"Les principes de l'assurance du risque cyber pour les compagnies maritimes"* , *op.cit,* p.3.
[350] *"L'I.A.C.S. établit d'une façon générale des exigences techniques ou administratives (Unified Requirements) auxquelles doivent satisfaire les règles particulières de ses membres, et des règles structurales communes (Common Structural Rules) dans certains cas (pétroliers à double coque, vraquiers)", in.,* Encyclopédie Universalis, https://www.universalis.fr/encyclopedie/societes-de-classification/, Consulté le 14/08/2023.
[351] IUMI, *"Insuring cyber risk"*, *in.,* Ship & offshore, n°5, 2017, p.42. Traduit par nous même.
[352] *Ibid.*
[353] PIETTE G, *" Le commerce maritime face au risque cyber"*, *op.cit.*, p.2.

Les sociétés de transport se sont aussi intéressées au sujet. La société DNV, entre autres, en développant la notation de classe *Cyber secure*, peut, désormais, répondre aux premiers aspects de la cybersécurité d'un navire et aux besoins opérationnels de l'armateur[354].

De surcroît, avec la création d'un nouvel organe bilatéral, "*le Groupe de coopération technique de l'IACS IUMI ",* l'industrie maritime peut discuter des questions telles que la cybersécurité et l'avenir du transport autonome, ce qui renforce encore la collaboration entre les sociétés de classification et les assureurs maritimes[355].

Par ailleurs, hormis ces solutions de couvertures proposées par les assurances et les P&I club, certains auteurs estiment que des solutions de réassurance étatique par des caisses détenues par l'Etat, peuvent être proposées dans le futur pour couvrir le risque cyber maritime.

Par exemple, faire appel, en France, à la *"caisse centrale de réassurance"* (CCR Re), détenue à 100% par l'Etat, reste aussi une solution envisageable[356].

"*La CCR Re présente la particularité de proposer, avec la garantie de l'Etat, des couvertures illimitées pour des risques exceptionnels, non assurables souscrits en France, qui naissent de l'utilisation de transport de toute nature ou se rapportent à des biens en cours de transport (ex: risque de guerre, actes terroristes…)"*[357].

A présent, avec les clauses d'exclusion du risque *marétique,* assez fréquentes dans les polices d'assurances privées, certains auteurs proposent de se tourner vers la couverture étatique. Cependant, d'autres voix s'élèvent pour mettre en exergue les limites de cette proposition.

En effet, l'Etat offre déjà la garantie des assurances obligatoires de dommages (FGAO) , la couverture des dommages résultant des catastrophes

[354] PIETTE G, *" Le commerce maritime face au risque cyber"*, *op.cit.*, p.2.
[355] IUMI, *"Insuring cyber risk"*, *op.cit.*
[356] QUASHIE F., ROLLAND E., SPINEC A., VALERO C., *"L'assurance maritime: évolution de la perception du risque"*, ISEMAR, note de synthèse, n° 192, septembre 2017, p.4.
[357] *Ibid*.

naturelles ou des actes terroristes[358]. Donc, si on arrive à assimiler un risque cyber à un acte de terrorisme , sous certaine conditions, la couverture étatique pourrait marcher.

Autrement dit, *" si des actes de terrorisme utilisant des méthodes numériques venaient à engendrer des dommages corporels et matériels, les mécanismes en place interviendraient normalement*"[359]. Par conséquent, dans l'hypothèse où un acte de terrorisme s'organise avec des moyens technologiques, le fonds agirait automatiquement en tant qu'assureur. Par contre, la question reste sans réponse pour ce qui des cyberattaques qui n'engendrent que des dégâts immatériels. En réalité, ces derniers constituent, malheureusement, la majorité des dommages causés par des cyber incidents.

In fine, il est certain qu'aujourd'hui, l'industrie d'assurance maritime offre une réponse mitigée sur la meilleure façon d'assurer la cybersécurité[360].

Certains assureurs maritimes, par exemple, veulent s'attaquer au risque d'accumulation et de systématicité qui découle potentiellement d'une cyberattaque et qui est susceptible d'avoir des conséquences beaucoup plus vastes[361]. D'autres, se limitent aux conséquences directes des cyber incidents.

Enfin, nous estimons que chaque situation doit être évaluée individuellement et les polices doivent être adaptées aux besoins particuliers du client. Les assureurs maritimes demeurent des fournisseurs de services - *service providers* et, collectivement avec d'autres organisations de l'industrie, il est clair qu'ils essaient d'unifier leur réponse face aux menaces cybernétiques[362].

A l'heure actuelle, comme l'a évoqué Fabien CAPARROS, conseiller digital et cybersécurité de la représentation française auprès de l'UE, lors du PARISMAT 2023, la progression de l'industrie maritime vers le chemin de la cybersécurité mérite d'être encouragée[363].

---

[358] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, p.102.
[359] 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",* Telecom, Paris Tech, 2017, p.68, note (188), *in.*, THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, p.102.
[360] IUMI, *"Insuring cyber risk"*, *op.cit.* p.43.
[361] *Ibid.*
[362] *Ibid.*
[363] CESAM, PARISMAT 2023, table ronde : *Comment l'écosystème maritime et aérien fait face à la montée du risque cyber ?*, *op.cit.*

Le fait de passer de la décennie de la protection, aux débuts des années 2000, avec les Firewalls et les antivirus, à la décennie de la détection avec la mise en place des logiciels de détection des menaces cyber, pour arriver aujourd'hui, à la décennie de la cyber résilience, est déjà une illustration de ce progrès[364]. Désormais, l'industrie essaie de bien préparer les crises au point de vue défensif et de travailler sur sa capacité d'anticipation, pour que l'impact des cyberattaques soit le moindre.

Dans le futur, des améliorations semblent être indispensables au développement de la cyber assurance maritime. Les difficultés liées à ce risque sont encore nombreuses, et des incertitudes quant à l'avenir de ce marché perdurent (section 2).

[364] CESAM, PARISMAT 2023, table ronde : *Comment l'écosystème maritime et aérien fait face à la montée du risque cyber ?*, *op.cit.*

Section 2 : L'avenir du marché d'assurance cyber maritime

L'avenir du marché d'assurance cyber maritime présente des défis et des opportunités considérables à mesure que la digitalisation numérique continue de s'étendre dans l'industrie maritime. Comme nous avons pu le voir tout au long de notre analyse, bien que les avantages de l'automatisation et des systèmes interconnectés soient indéniables, ils exposent également les acteurs de ce secteur à des risques cybernétiques croissants.

Donc, considérer que l'on pourrait être épargné des cyberattaques est une erreur à ne plus commettre[365]. A présent, l'industrie maritime est en train d'évoluer vers une culture où l'apprentissage des erreurs joue un rôle central dans la protection de ce risque.

Le futur du marché cyber n'est certes pas tout tracé, mais, désormais, les signaux sont de plus en plus positifs, ce qui nous permet d'affirmer qu'il y aura certainement un avenir prometteur[366].

Quoi qu'ils existent encore des problèmes non résolus qui peuvent freiner le développement de l'assurance cyber maritime (A), il est important de reconnaître aussi les progrès significatifs, qui ont été déjà accomplis dans ce domaine (B)

A)- Des problèmes non résolus dans l'évaluation des cyber-sinistres maritimes

Aujourd'hui, avec le développement des nouvelles technologies numériques, plusieurs questions émergent et les spécialistes ont davantage du mal à y répondre. Le cyber risque étant insaisissable et constamment évolutif, laisse toujours la porte ouverte à l'apparition de nouvelles problématiques.

---

[365] NOTIN J., *"Autopsie des cyberattaques et des moyens de s'en protéger par le dispositif national de prévention et d'assistance Cybermalveillance.gouv.frs", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.101.
[366] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, *op.cit.,* p.109.

A ce stade, *"nous n'en sommes qu'au début. Les progrès technologiques dans le secteur du transport maritime, comme les navires autonomes, les drones et diverses applications utilisant les blockchains, sont particulièrement prometteurs pour l'offre de transport maritime mais les acteurs du secteur restent incertains notamment quant aux risques de cybersécurité"*[367].

De ce fait, parallèlement aux innovations technologiques et au développement numérique constant dans l'industrie maritime, les obstacles liés à l'assurabilité des menaces cyber maritimes risquent de devenir plus prégnants.

Nous nous intéresserons dans cette partie à, principalement, deux défis, qui peuvent croiser le chemin des assureurs, en couvrant le risque cyber maritime : en premier lieu, les difficultés relatives à la délimitation de la responsabilité avec l'apparition des navires autonomes (1), en deuxième lieu, les difficultés de quantification souvent rencontrés dans la délimitation des taux de primes et des coûts d'indemnisation (2).

1. Difficultés dans la détermination du responsable : l'exemple des navires sans équipage

A priori, il semblerait peut-être *"...prématuré de lier les sujets de cybersécurité et de navire sans équipage, mais ce sont aujourd'hui des thèmes qui ne peuvent plus être étudiés séparément. Leur analyse conjointe se voit justifiée par la place qu'a pris aujourd'hui le cyber-risque"*[368].

Pour commencer, il faut déjà souligner que l'appellation navire sans équipage, recouvre deux divisions de navires. *"...Il est nécessaire de bien distinguer le navire guidé à partir d'une salle de contrôle à terre de celui totalement autonome"*[369]. Nous trouvons d'une part, des navires sans équipage,

[367] AUBERGER C., *"Cybersécurité maritime, un enjeu stratégique pour tous les acteurs de la filière"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.13.
[368] LASMOLES O., *"Cybersécurité et navires sans équipage"*, *op.cit.,* p.777.
[369] *Ibid.,* p.772.

commandés à distance, à partir de la terre, grâce à des caméras et micros installés à bord[370] et d'autre part, des navires 100% autonomes. Ces derniers, grâce au procédé du *deep learning,* basé sur l'apprentissage par expérience, sont censés pouvoir améliorer la sécurité de navigation et éviter près de 80 % des accidents maritimes[371].

En Droit français, le code des transports, dans son article L5000-2-1, évoque également ces deux types de navires sans équipage. Il considère le navire autonome comme : *"...un navire opéré à distance ou par ses propres systèmes d'exploitation, qu'il y ait ou non des gens de mer à bord…".*

Ainsi, se pose, inévitablement, la question de détermination du responsable en cas d'incident, sur ces deux catégories de navires sans équipage.

De prime abord, dans l'hypothèse d'un dommage causé à un navire téléguidé depuis la terre, c'est la responsabilité de la personne en charge du pilotage à terre, qui serait engagée, ou de son commettant s'il n'est qu'un préposé[372]. Dans ce contexte, l'article 1242 du code civil français[373] pose le principe de la responsabilité des choses que l'on a sous sa garde. Selon les termes de cet article, toute personne chargée de l'usage, la gestion ou du contrôle d'un bien, est présumée responsable en cas de dommage.

La possibilité d'engager la responsabilité du fabricant des capteurs embarqués ou du système de transmission de données, reste également envisageable en cas de défaillance technique[374].

Pour ce qui est des navires totalement autonomes, la question de responsabilité se révèle plus délicate. "*Le navire traite par lui-même les données collectées par ses capteurs, prend ses décisions et optimise son*

[370] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, *in.,* Transport et sécurité, LexisNexis, 2019, p.320.
[371] *Ibid.*
[372] *Ibid.*, p. 325.
[373] Article 1242 code civil français, tel que modifié par l'ordonnance n°2016-131 du 10 février 2016, dispose : " *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde…",* https://www.legifrance.gouv.fr/, Consulté le 15/08/2023.
[374] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies" op.cit.,* p.325.

trafic"[375]. Qui serait donc responsable en cas d'accident ? Est-ce l'armateur, le créateur du programme ou le vendeur de ce dernier ?

Dans l'hypothèse d'un accident causé par un navire totalement autonome, il est évident que l'armateur, en tant qu'exploitant du navire, sera en première ligne[376]. En effet, il s'agit ici de la simple application d'un principe juridique classique qui fait peser la responsabilité dans un premier plan, à celui qui exploite, utilise, ou tire profit d'une chose[377].

Toutefois, on pourrait aussi imaginer un scénario où les responsabilités de l'armateur, du concepteur du programme et celle de son vendeur seraient combinées. Une situation pareille entraînera certainement un partage de responsabilités, parfois complexe[378].

Une autre position, qui peut sembler poétique pour certains, plaide en faveur d'une responsabilité du robot, en l'occurrence celle du navire autonome. *"Se retrouve ici l'idée que le navire doit répondre lui-même de ses dettes"*[379]. Aurait-il à cet effet une personnalité juridique distincte de celle de la personne qui l'utilise ou en tire profit ?

A ce niveau, la position du Parlement Européen se révèle assez intéressante[380].

Il *"... préconise en effet un cadre de responsabilité civile qui rendrait les personnes ayant recours à l'intelligence artificielle à haut risque responsables de tout dommage résultant de son utilisation*"[381].

---

[375] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies" op.cit.,* p.326.
[376] PIETTE G., Traité du Droit maritime, *op.cit.*, p.885.
[377] *Ibid.*
[378] *Ibid.*
[379] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies" op.cit.,* p.326.
[380] Résolution du Parlement Européen contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)), 16 février 2017, *" ...Responsabilité. Z. considérant que, grâce aux impressionnants progrès technologiques au cours des dix dernières années, non seulement les robots contemporains sont capables de mener à bien des tâches qui relevaient autrefois exclusivement de la compétence humaine, mais encore que la mise au point de certaines fonctionnalités autonomes et cognitives (comme la capacité de tirer des leçons de l'expérience ou de prendre des décisions quasi-indépendantes) rapprochent davantage ces robots du statut d'agents interagissant avec leur environnement et pouvant le modifier de manière significative; que, dans un tel contexte, la question de la responsabilité juridique en cas d'action dommageable d'un robot devient une question cruciale…".*
[381] PIETTE G., Traité du Droit maritime, *op.cit.*, p.885.

Il soutient même l'idée de créer une personnalité juridique spécifique aux robots autonomes et les considère comme des personnes électroniques responsables en cas de dommage[382].

A présent, cette doctrine de personnalité juridique des robots demeure encore peu réalisable, notamment dans le cadre du Droit français qui tient encore à la division radicale entre "personnes" et "choses"[383].

Intimement liée à la responsabilité, l'assurance se voit, aussi réticente quant à la nouveauté de cette invention et des risques qui peuvent découler de sa mise en service. Certains de l'industrie assurantielle se rendent compte rapidement que, même si la nouveauté rend l'évaluation du risque difficile, la sécurité et la sûreté que cette technologie promet, contribueront indubitablement à réduire les risques maritimes de toutes sortes[384]. En cas de sinistre sérieux, les dommages seront moindres, vu qu'il n'y aura personne à bord, d'où aucune perte humaine[385].

D'autres auteurs de l'industrie expriment un avis totalement contraire vis-à-vis de l'assurabilité des navires sans équipage, au point d'estimer 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"*[386].

Concrètement, pour pouvoir couvrir un navire avec une police d'assurance maritime, les assureurs vont regarder essentiellement, si celui-ci est en bon état de navigabilité.

La notion de navigabilité, telle qu'évoquée dans la Convention de Bruxelles de 1924[387], repose sur trois piliers dont l'un est relatif à l'équipage du navire. Celui-ci doit disposer d'un équipage adéquat et compétent à son bord.

---

[382] Résolution du Parlement Européen contenant des recommandations à la Commission concernant des règles de Droit civil sur la robotique (2015/2103(INL)), 16 février 2017, (59.f).
[383] *Cf.,* PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies" op.cit.,* p.326.
[384] KEGELS A., *" Le transport autonome sur les voies navigables intérieures",* DMF, n°829, 1er novembre 2020, p. 3.
[385] *Ibid.*
[386] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, *op.cit.*, p.52.
[387] Convention internationale pour l'unification de certaines règles en matière de connaissement, Conclue à Bruxelles le 25 août 1924, modifiée par le protocole du 23 février 1968 et par le protocole du 21 décembre 1979.

En l'absence d'un tel équipage, le navire est considéré comme étant en état d'innavigabilité[388].

Par ailleurs,"*sans interprétation et adaptation du droit maritime, les navires sans équipage ne satisferont pas à l'exigence de navigabilité"*[389].

Dans ce même ordre d'idées, l'assuré est tenu, en cas d'incident, de prendre toutes les mesures nécessaires, afin de limiter et éviter l'aggravation du dommage[390]. N'étant pas à bord, l'accomplissement de cette responsabilité devient impossible.

Enfin, avec le navire sans équipage, l'éventualité de production de cyberattaques va sans doute augmenter. Comme on l'a vu tout au long de notre analyse, les assureurs maritimes ont l'habitude d'exclure le risque cyber. Par contre, s'il est question de navires sans équipage, cette exclusion devient absurde et ne serait plus adaptée aux besoins d'une navigation, de plus en plus automatisée[391].

"Ainsi, émerge, dans le brouillard d'une digitalisation galopante et dans le spectre potentiel du navire autonome ou du navire sans équipage, le concept flou de cyber-navigabilité"[392].

Ce concept serait probablement déterminé grâce aux sociétés de classification. Ces dernières, depuis longtemps, jouent un rôle primordial dans la certification des navires et la délivrance des titres de sécurité.

Nous pensons, donc, que la position des assureurs et celle des P&I Clubs, sera fondée en amont, sur la décision des sociétés de classification[393].

A cet égard, dans le cas où ces entités devaient refuser d'émettre les certificats de sécurité ou de classer les navires sans équipage, les assureurs s'abstiendront d'offrir leur couverture[394].

---

[388] CHESNEAU A., *"Les "navires autonomes ". Enjeux et impacts d'une navigation sans équipage dans le monde maritime"*, HAL Open science, Droit, 22 janvier 2018, p.74, https://dumas.ccsd.cnrs.fr /dumas -01622 134/d, Consulté le 15/08/2023.
[389] *Ibid.*
[390] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, *op.cit.*, p.52.
[391] CHESNEAU A., *"Les " navires autonomes ". Enjeux et impacts d'une navigation sans équipage dans le monde maritime"*, *op.cit.,* p.74.
[392] MANET F.-C., *"La marétique, un enjeu essentiel pour l'humanité ?"*, *op.cit.*, p.89.
[393] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies" op.cit.,* p. 328.
[394] *Ibid.*

Jusqu'à présent, pour les assureurs maritimes, les polices types corps et facultés ne prennent pas en compte les navires sans équipage[395]. Dans l'avenir, il serait indubitablement intéressant de voir la réaction de l'industrie assurantielle maritime, quand le recours à ces navires sera plus démocratisé.

Quant aux P&I Clubs, désormais, ils se penchent davantage sur les questions de cybersécurité des navires, sans encore aborder l'impact qu'auraient les navires sans équipage sur ce sujet. Pour le moment, le seul à traiter cette problématique est le *Shipowners Club,* qui a élaboré une police spéciale : *Maritime autonomous vessel liability insurance,* focalisée sur les navires sans équipage de petite taille[396].

Dans cette dynamique en constante évolution, la perspective adoptée par les assureurs et les P&I clubs à l'égard des navires sans équipage revêt d'une importance cruciale dans le façonnement de l'avenir de la navigation autonome.

En l'absence d'une assurance adéquate, les acteurs de l'industrie, qu'ils s'agissent de fabricants, d'opérateurs, de fournisseurs de technologies, ou encore d'armateurs, pourraient hésiter à adopter le transport autonome en raison de la responsabilité accrue et des conséquences financières potentiellement importantes en cas d'incident.

Certes, dans le futur, l'assurance jouera un rôle crucial dans la facilitation de l'acceptation et de l'adoption des technologies autonomes dans notre société moderne en général, mais elle contribuera, plus particulièrement, à créer un environnement réglementaire favorable à leur intégration réussie dans l'industrie maritime.

Ayant clôturé notre premier paragraphe portant sur les défis relatifs à la responsabilité, que peut soulever le recours aux navires sans équipages, nous entamerons notre second paragraphe, sur les difficultés que rencontrent les

[395] PIETTE G., Traité du Droit maritime, *op.cit.*, p.889.
[396] *Ibid.*

assureurs maritimes dans la quantification des taux d'indemnisations et des primes, s'agissant du risque cyber maritime (2).

2. Difficultés dans la délimitation du taux d'indemnisation et les taux de primes

L'un des principes fondamentaux en assurances est celui de la mutualisation des risques. Ce principe sous-tend l'idée que les assureurs sont capables de prévoir la perte moyenne par assuré, en appliquant ce qu'on appelle la *"loi du plus grand nombre"*[397].

Selon cette loi, même si les indemnités versées aux assurés, en cas de sinistre, sont soumises à des aléas, elles tendent à rester relativement constantes, lorsque les dommages sont répartis de manière équitable et indépendante entre les assurés[398]. En d'autres termes, si de nombreux individus souscrivent à une assurance, les coûts liés aux sinistres de quelques-uns seront répartis sur l'ensemble des participants.

Ainsi, les primes versées par tous les assurés vont contribuer à couvrir les pertes subies par ceux qui ont été touchés par un sinistre.

La nature particulière et systémique du cyber risque remet en question cette conception classique de mutualisation. Contrairement aux risques habituels traditionnels, où les sinistres sont souvent indépendants, la cybermenace conduit le plus souvent, à la production d'une chaîne d'attaques qui peut se propager rapidement d'un système à un autre.

Dans ce sens, selon une enquête menée par le groupe Zurich assurances[399], il est suggéré que certaines attaques cybernétiques pourraient potentiellement déclencher un impact systémique similaire à celui observé durant la crise financière de 2008, en ciblant les infrastructures informatiques

[397] THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, *op.cit.*, p.58.
[398] *Ibid.*
[399] BAUME T., " *Cyber - risques : les difficultés des assureurs pour apporter la bonne réponse",* L'Argus de l'assurance, 25 juin 2014, https://www.argusdelassurance.com/risk-management/cyber-risques-les-difficultes-des-assureurs-pour-apporter-la-bonne-reponse.79683, Consulté le 19/08/2023.

internes des entreprises, les services de *cloud computing*[400] et les chaînes d'approvisionnement.

Un exemple récent qui met en exergue cette interdépendance des risques est l'attaque par *"...le logiciel malveillant NotPetya, qui s'est servi de la procédure de mise à jour d'un logiciel de comptabilité ukrainien pour infecter diverses cibles en Ukraine, dont l'aéroport de Kiev ainsi que le système de surveillance des radiations de la centrale nucléaire de Tchernobyl, avant de contaminer la Russie, le Royaume-Uni, la Norvège, les Pays-Bas ou la France, le 27 juin 2017, seulement cinq heures après la première détection du virus"*[401].

Cette corrélation entre plusieurs risques cyber pose un défi majeur aux assureurs, celui de sa quantification. A ce titre, la délimitation de la prime à payer par l'assuré et des taux d'indemnisation, deviennent des tâches complexes.

Dans ce contexte, tel que précisé dans un rapport publié par l'OCDE[402], plusieurs facteurs peuvent influencer la prime d'assurance, notamment le niveau d'incertitude dans l'estimation des pertes prévues, ce qu'on appelle la *"quantifiabilité",* l'ampleur des pertes prévues ou la viabilité économique pour l'assurance et enfin la diversité de l'ensemble des risques couverts, c'est à dire la corrélation limitée.

Il va sans dire que l'assurance de la menace cyber serait problématique sur ces trois niveaux, mais, les difficultés à quantifier un risque relativement nouveau et évolutif, tel que le risque cyber, et la possibilité d'une corrélation significative entre les assurés, d'où un risque d'accumulation, demeurent les défis les plus critiques dans la souscription du cyber risque[403].

---

[400] Selon la CNIL, le Cloud Computing : *"... (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (cloud) composé de nombreux serveurs distants interconnectés"*, https://www.cnil.fr/fr/definition /cloud-computing, Consulté le 20/08/2023.

[401] LE CLUB DES JURISTES, "*Rapport : Assurer le risque cyber"*, Tome 1, Janvier 2018, p.25.

[402] OECD, *"Enhancing the Role of Insurance in Cyber Risk Management"*, OECD Publishing, 2017, Paris, p.94.

[403] *Ibid.*

Pour ce qui est de la la *"quantifiabilité",* sur les 36 répondants du secteur de l'assurance au questionnaire de l'OCDE portant sur les défis liés à l'extension de la couverture des cyberrisques, près des deux tiers considèrent la capacité de quantifier la cyber exposition comme une préoccupation majeure[404].

Selon ce même rapport, trois défis pourraient faire obstacle à la quantification du risque cyber.

Dans un premier temps, il s'agit de la disponibilité limitée, voire l'absence des données historiques relatives à la cybermenace. Bien que les attaques cyber dans le domaine maritime aient augmenté ces dernières années, il existe peu d'informations recueillies concernant leurs sources et leurs niveaux d'ampleur[405]. Ce manque de données rend la tâche des assureurs maritimes plus difficile lorsqu'il s'agit d'établir les tarifs appropriés[406].

L'absence de mécanismes de mesure du risque engendre une réelle complexité s'agissant de la délimitation des tarifs d'assurance cyber[407].

"Concrètement, cela se traduit par une segmentation tarifaire limitée peu propice à une croissance forte de la souscription de ce type de garantie"[408].

Cette insuffisance de données se voit exacerbée par la réticence générale des victimes d'incidents cybernétiques à partager des informations sur ces événements et leur impact, à moins que cela ne soit nécessaire, par crainte de répercussions sur leur réputation[409].

Ensuite, le changement constant des cyberrisques pose également problème pour la délimitation des tarifs d'assurance. En effet, même si ces données étaient disponibles, elles pourraient devenir rapidement désuètes en raison de l'évolution rapide des cyberrisques. Les cybercriminels continueraient à améliorer leurs méthodes d'attaque et à trouver de nouvelles façons d'échapper à la cybersécurité.

---

[404] OECD, *"Enhancing the Role of Insurance in Cyber Risk Management"*, *op.cit.,* p.94.
[405] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.74.
[406] *Ibid.*
[407] DREYFUSS M.-L., La révolution digitale dans l'assurance*, op.cit.*, p.68.
[408] *Ibid.*
[409] OECD, *"Enhancing the Role of Insurance in Cyber Risk Management", op.cit.,* p.94.

Quant au risque d'accumulation, les assureurs seraient ici aussi confrontés à délimiter les frontières entre plusieurs catégories d'assurances (telles que les assurances pour les dommages matériels, les pertes d'exploitation, les accidents du travail, la responsabilité civile, etc.), qui peuvent être impactées simultanément par le risque cyber. En d'autres termes, ces incidents peuvent déclencher des demandes de remboursement et de réparation dans divers domaines de l'assurance en même temps[410].

En somme, dans le cas des risques cybernétiques, la corrélation des pertes entre les assurés à travers différents types de couvertures est fort probable. De plus, "*la diversification géographique des risques souscrits est… inopérante puisque les incidents cyber peuvent être transfrontières"*[411]. Contrairement à d'autres périls, il est plus difficile de constituer un ensemble diversifié de risques en fonction de la délimitation géographique ou même du secteur d'activité, compte tenu des rapports interreliés des infrastructures, logiciels et services[412], dans le secteur industriel en général et le secteur maritime plus particulièrement.

Selon certains rapports, cette potentielle accumulation constitue la principale raison pour laquelle les assureurs limitent la couverture des cyber risques ou les excluent carrément[413].

Face à la recrudescence de la cyber menace *"le monde entier devient une zone de cumul"*[414] de risques.

Pour conclure, il est à noter qu'à ce stade de développement du marché de la cyber assurance, le manque d'informations historiques et l'accumulation potentielle des risques entravent son progrès[415]. De son côté, la capacité des assureurs à déterminer des primes précises prenant en compte des particularités du profil de l'assuré, se voit aussi limitée.

---

[410] LE CLUB DES JURISTES, "*Rapport : Assurer le risque cyber"*, *op.cit.*, p.26.
[411] *Ibid*.
[412] OECD, *"Enhancing the Role of Insurance in Cyber Risk Management", op.cit.,* p.96.
[413] *Ibid.*
[414] JAGHADAM A., *"Les conditions d'assurabilité des cyber-risques"*, Revue Risque, n°. 77, 2009, *in.*, LE CLUB DES JURISTES, "*Rapport : Assurer le risque cyber"*, *op.cit.,* p.26, note (5).
[415] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.75.

A cet égard, "*le secteur doit clairement rattraper son retard et un effort important d'évangélisation et de sensibilisation est impératif*"[416].

Pour ce fait, les assureurs doivent prendre en compte cette réalité unique et complexe de la menace cyber. Les modèles traditionnels de tarification et de gestion des risques peuvent nécessiter des ajustements importants pour tenir compte de la nature interconnectée de ces nouveaux risques.

Les assureurs doivent donc repenser leurs approches pour évaluer, tarifer et gérer les risques cybernétiques.

En dépit de tous ces défis persistants, les progrès accomplis dans le domaine de la cyber assurance, en particulier dans le secteur maritime, témoignent de la capacité de l'industrie à s'adapter et à innover pour faire face aux menaces cybernétiques. Les avancées réalisées et celles à venir présagent un avenir où l'assurance cyber maritime deviendra un élément essentiel de la stratégie de gestion des risques pour les différents acteurs maritimes (B).

Tirer des leçons des erreurs antérieures favorisera, certes, une industrie plus résiliente, adaptable et axée sur la sécurité, qui façonnera un avenir maritime plus durable et efficace.

[416] AUBERGER C., *"Cybersécurité maritime, un enjeu stratégique pour tous les acteurs de la filière"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p.13.

B) - Des progrès pour le marché d'assurance cyber maritime

On ne peut nier que la conclusion d'un contrat d'assurance est une condition sine qua none à la réalisation de l'opération de transport maritime. Mais, au regard de la digitalisation accrue de ce secteur, les assureurs seraient amenés à adapter certains concepts intrinsèques à l'assurance, afin de permettre une meilleure adaptabilité aux potentiels risques futurs.

A cet égard, l'avenir du marché d'assurance maritime dépendra de la réaction des ses acteurs face au développement des nouvelles technologies.

Si ces derniers seraient favorables à l'adoption de ces inventions dans leur système, l'industrie assurantielle serait amenée à réformer ses réglementations afin d'anticiper les risques qui pourraient découler de l'usage des technologies numériques.

A priori, la réaction des acteurs maritimes semble être positive. L'usage des nouvelles technologies dans ce secteur, devient la pierre angulaire d'un commerce maritime moderne.

Dans le futur, certaines de ces inventions vont révolutionner le commerce maritime et permettront un gain de temps et de productivité considérable.

Selon le Pr Gaël PIETTE, ces progrès technologiques viseraient principalement à renforcer d'un côté la sécurité maritime des navires, et d'un autre la sécurité juridique[417].

En ce qui concerne la sécurité maritime, les avancées à venir seront fondées principalement sur l'intelligence artificielle (IA). Celle-ci aurait un impact significatif tant sur le développement des navires autonomes, que sur la mise en service des *smart ports* et des *smart containers*[418].

Les années à venir seront aussi marquées par des progrès visant la sécurisation juridique du secteur. Le connaissement électronique est l'une de

[417] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, *in.,* Transport et sécurité, LexisNexis, 2019, p.318.
[418] *Ibid.*

ces inventions qui sert déjà et va servir encore dans le futur à la sécurisation des contrats maritimes[419].

Produit de l'essor des nouvelles technologies, le connaissement électronique ou plutôt le connaissement dématérialisé[420], suscite l'intérêt de l'industrie du commerce maritime, qui cherche davantage, dans le cadre d'une mondialisation croissante, à économiser sur les coûts de transport et à gagner en productivité.

Sur un plan pratique, le connaissement électronique permet d'éviter nombreuses difficultés qu'un transporteur maritime pourrait rencontrer en utilisant des connaissements papiers.

La facilité de le modifier permettra, de toute évidence, de réduire l'erreur, en offrant la possibilité de changer des détails relatifs au transport ou à la marchandise, tout au long du voyage[421].

Par contre, d'un point de vue juridique, aucune définition, claire du connaissement électronique, n'a été donnée.

Pour autant, en Droit français, grâce aux lois du 13 mars 2000[422] et du 21 juin 2004[423], une valeur juridique a été attribuée aux documents électroniques, parmi lesquels s'inscrit le connaissement dématérialisé[424].

En Droit international, deux textes méritent d'être mentionnés[425] : les règles du Comité Maritime International (CMI) relatives aux connaissements électroniques[426] et les règles de Rotterdam[427].

"*Le procédé imaginé par les règles élaborées par le CMI au sujet des connaissements électroniques repose sur la création d'une clé électronique*

---

[419] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, op.cit., p.321.
[420] PIETTE G., Traité du Droit maritime, 2023, *éd.,* Pedone, p.698.
[421] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, *op.cit.*, p.321.
[422] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62 du 14 mars 2000.
[423] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004.
[424] PIETTE G., Traité du Droit maritime, *op.cit*., p.698.
[425] *Ibid*., p.699.
[426] CMI, Rules for electronic bills of lading, juin 1990, https://comitemaritime.org/work/rules- for-electronic-billing-of-lading/, Consulté le 23/08/2023.
[427] Convention des Nations Unies sur le contrat de transport international de marchandises effectué entièrement ou partiellement par mer, Règles de Rotterdam, New York, 11 décembre 2008, https://uncitral.un.org/sites /uncitral .un.org/files/media-documents/uncitral/fr/rotterdam-rules-f.pdf, Consulté le 23/08/2023.

codée (private key) qui regroupe les données relatives au transport, remise au chargeur"[428]*,* par le transporteur.

De ce fait, dans l'hypothèse où la marchandise transportée serait vendue au cours du voyage, avant l'arrivée à destination, le transfert du connaissement s'effectuera par l'annulation de la clé initiale et la génération d'une nouvelle clé au nouveau porteur[429].

Ce procédé de transfert du connaissement semble être plus fiable et sécurisé en comparaison avec la méthode traditionnelle de transmission des documents. En revanche, ces règles du CMI restent dépourvues de toute valeur contraignante[430], ce qui implique que les parties ne seront pas obligées de les respecter.

De leur côté, les règles de Rotterdam ne traitent pas directement du connaissement électronique, mais évoquent plutôt le document électronique de transport. Selon l'article 1.18 de cette convention, le terme *"document électronique de transport"* fait référence à *: "... l'information contenue dans un ou plusieurs messages émis au moyen d'une communication électronique par un transporteur en vertu d'un contrat de transport, y compris l'information qui est logiquement associée au document sous la forme de données jointes ou y est autrement liée au moment de son émission par le transporteur ou ultérieurement de manière à en faire partie intégrante, qui: a) Constate la réception, par le transporteur ou une partie exécutante, des marchandises en vertu du contrat de transport; et b) Constate ou contient le contrat de transport".*

Ce même texte pose un principe fondamental *"...qui es*t *l'équivalence des effets entre le connaissement électronique et le connaissement papier"*[431]. D'après les dispositions de l'article 8.b de cette convention *: " L'émission, le contrôle exclusif ou le transfert d'un document électronique de transport a le même effet que l'émission, la possession ou le transfert d'un document de*

[428] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*, *op.cit.*, p.321.
[429] *Ibid.*
[430] PIETTE G., Traité du Droit maritime, *op.cit.,* p.699.
[431] *Ibid.,* p.700.

transport". Le connaissement électronique se voit ainsi sur un même pied d'égalité qu'un connaissement papier.

En résumé, la généralisation, à long terme, du connaissement électronique dans les échanges commerciaux va contribuer au changement radical de leur nature dans le monde maritime. En revanche, bien que perçu depuis de nombreuses années comme le futur de l'industrie maritime[432], des atténuations doivent être apportées, quant à l'efficacité de cet instrument.

En effet, certains doutent de la négociabilité de ce document notamment au regard des relations avec les tiers[433]. D'autres craignent une potentielle augmentation des menaces cybernétiques, particulièrement, avec un recours plus fréquent aux connaissements électroniques.

A ce niveau, il est indubitable que, plus, les nouvelles technologies intègrent les rapports commerciaux du monde maritime, plus, l'éventualité de production des risques cybernétiques serait accrue.

A cet égard, les P&I Club ont prévu des clauses spécifiques au connaissement électronique qui excluent sa prise en charge, dans le cas où le mécanisme électronique permettant d'utiliser ce document, n'a pas reçu l'approbation préalable par le club de protection[434].

Compte tenu de ces risques, la *blockchain* pourrait se présenter comme un espoir pour la sécurisation des données, y compris celles inscrites dans les connaissements électroniques.

Se basant sur des principes fondamentaux tels que la décentralisation, la transparence et la cryptographie, la *blockchain* offre la possibilité de créer des registres inviolables et immuables. Toutes ces caractéristiques pourraient se révéler particulièrement pertinentes pour protéger les données sensibles, notamment celles des connaissements électroniques.

Dans cette perspective, les acteurs du transport maritime se voient porter de plus en plus leur attention sur la *blockchain*. Ils y trouvent une grande sécurité et de la transparence dans les transactions[435].

---

[432] LOOTGIETER S., *"Les risques cybernétiques dans le domaine des transports"* , DMF n° 775, 8 décembre 2015, p.2.
[433] PIETTE G., *"La sécurité en droit maritime à l'épreuve des nouvelles technologies"*,
[434] *Ibid.*
[435] MATCHINDA O., *"La dématérialisation des documents de transport maritime de marchandises : (Étude dans le cadre de la CEMAC)",* Thèse de doctorat, Université Paris 1 Panthéon Sorbonne, 09 février 2021, p.310.

Mais d'abord, avant de recenser les avantages de cette technologie et ce qu'elle peut offrir au monde maritime, il faut essayer de la définir.

Selon la CNIL, il s'agit d'*"une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle"*[436].

La mission d'information commune de l'Assemblée nationale française, quant à elle, considère la *blockchain* comme *"un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie"*[437].

Ces diverses définitions convergent vers un élément commun : le caractère sécurisé, décentralisé et distribué de la *blockchain*[438].

On parle même d'inviolabilité du mécanisme de la *blockchain*, puisqu'il est impossible de modifier l'historique des opérations enregistrées et difficile de pirater le système, grâce à la distribution des données sur différents ordinateurs participants[439].

En effet, bien que le droit maritime n'ait pas encore pleinement exploré les différentes implications de la technologie *blockchain*, les acteurs du domaine des transports portent un intérêt sérieux à cette innovation.

A titre d'exemple, les assurances transport recourent, de plus en plus aux *smart contracts*[440] créés sur le registre *blockchain*, qui leur garantit une rapidité de service, une réduction des déplacements et une baisse des coûts

---

[436] CNIL, Commission nationale de l'informatique et des libertés, site officiel, https://www.cnil.fr/fr/definition/ blockchain, Consulté le 24/08/2023.

[437] Assemblée Nationale, *"Rapport de la mission d'information commune sur la blockchain (chaîne de blocs) et ses usages : un enjeu de souveraineté"*, décembre 2018, p.1., https://www2.assemblee-nationale.fr/static/15/ commissions /CFinances/blockchain-synthese.pdf?v=1692355067, Consulté le 24/08/2023.

[438] MATCHINDA O., *"La dématérialisation des documents de transport maritime de marchandises : (Étude dans le cadre de la CEMAC)", op.cit.,* p.310.

[439] PIETTE G., Traité du Droit maritime, *op.cit.*, p.869.

[440] Smart contracts : *"Les protocoles informatiques qui facilitent, vérifient et exécutent automatiquement la négociation d'un contrat d'assurance. L'objectif est d'améliorer la qualité de service offerte aux clients ainsi que leur visibilité sur leurs expositions aux risques encourus"*, *in.*, REMY M., "*La blockchain au service de l'assurance maritime"*, L'Argus de l'Assurance, 08 novembre 2018, https:// www. argusdelassurance .com / tech/la-blockchain-au-service-de-l-assurance-maritime.136654, Consulté le 24/08/2023.

relatifs aux traitements des dossiers papier et à la fraude, ce qui contribuera à l'amélioration de la procédure et à la compétitivité de l'entreprise[441].

A cet effet, un exemple concret nous vient à l'esprit, étant celui de l'assurance au voyage dans le transport aérien[442]. Dans une telle hypothèse, le contrat intelligent stocké sur la *blockchain*, va s'associer à des données disponibles sur le portail de l'entreprise, dans lequel les conditions générales du contrat seront enregistrées et exécutées de manière automatique[443].

Ainsi, s'il est enregistré que l'assuré sera indemnisé au bout de trente minutes de retard, l'opération sera faite automatiquement dès que cette condition est remplie[444].

De ce fait, et tel que Hélène STANAWAY, digital leader chez Axa XL, l'a rappelé, cette technologie favorise le *"...suivi en direct [qui]… permettra d'automatiser un certain nombre de tâches critiques et de proposer des solutions d'assurance globalement moins chères avec des couvertures mieux adaptées aux besoins réels ... [des] clients, notamment grâce à des surprimes au coup par coup ajustées à leur prise de risques*" [445].

Outre l'automatisation de la procédure, la *blockchain* se présente, également, comme l'une des meilleures solutions, face à la multiplication des menaces cyber, ce qui suscite le plus d'intérêt dans notre contexte.

Concrètement, la capacité de la *blockchain* à classer les données dans des *"conteneurs numériques"* pourrait constituer une révolution dans la maîtrise des cyber risques, aussi bien pour les compagnies maritimes que pour les assureurs[446].

Dans cette optique, un partenariat entre l'armateur MAERSK et la société IBM, s'est construit, en 2017, afin de développer une blockchain

---

[441] Ministère de l'économie des finances et de la souveraineté industrielle et numérique, *"Qu'est ce qu'une chaîne de blocs (blockchain) ?",* Bercy Info, 12 avril 2022, https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application, Consulté le 24/08/2023.

[442] MATCHINDA O., *"La dématérialisation des documents de transport maritime de marchandises : (Étude dans le cadre de la CEMAC)", op.cit.,* p.323.

[443] *Ibid.*

[444] *Ibid.*

[445] REMY M., "*La blockchain au service de l'assurance maritime"*, L'Argus de l'Assurance, 08 novembre 2018, https:// www. argusdelassurance.com/tech/la-blockchain-au-service-de-l-assurance-maritime.136654, Consulté le 24/08/2023.

[446] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.,* p.77.

nommée *TradeLens*[447]. Il est question d'une plateforme de chaîne d'approvisionnement ouverte et neutre soutenue par la technologie *blockchain.* Elle favorise le véritable partage d'informations et la collaboration entre les chaînes d'approvisionnement, ce qui permet d'accroître l'innovation de l'industrie, de réduire les frictions commerciales et, enfin, promouvoir davantage le commerce mondial[448].

Depuis sa création, *"...une centaine d'autorités portuaires (Bilbao, Halifax, Houston par exemple), d'entreprises, de transporteurs (tels que Canadian National Rail, MSC, CMA CGM, Hapag Lloyd, etc.) ou encore d'organismes publics (par exemple, les douanes américaines) ont rejoint cette blockchain"*[449].

En somme, tel que souligné par Shaun CRAWFORD, global vice chair of industry chez EY, la piste de la *blockchain,* ne se limitant plus à une simple numérisation, elle va, dans l'avenir, *"...introduire l'arrivée du produit d'assurance en temps réel qui pourra enfin couvrir les risques les plus incertains et complexes*"[450].

Cependant, il est important de noter que la mise en œuvre de la *blockchain* dans le secteur maritime n'est pas sans défis. Des questions liées à la réglementation, à l'interopérabilité des systèmes et à l'acceptation générale de cette technologie devraient être abordées, pour que la *blockchain* puisse atteindre son plein potentiel.

L'inviolabilité et l'infaillibilité de cette technologie restent partielles. *"Ici comme partout ailleurs, ni le risque zéro, ni la sécurité totale et absolue n'existent"*[451].

Par ailleurs, écarter certaines étapes, notamment dans la conclusion des contrats maritimes d'assurance, pour économiser en temps et en argent, pourrait être problématique. Il est essentiel de toujours faire preuve de

[447] PIETTE G., Traité du Droit maritime, *op.cit.*, p.870.
[448] *Cf.*, IBM, *"Présentation client de la plateforme TradeLens",* 17 avril 2019, https://www.ibm.com/downloads /cas /XNGVO4AY, Consulté le 25/08/2023.
[449] PIETTE G., Traité du Droit maritime, *op.cit.*, p.870.
[450] REMY M., "*La blockchain au service de l'assurance maritime"*, *op.cit.*.
[451] PIETTE G., Traité du Droit maritime, *op.cit.*, p.872.

prudence en évitant d'aller trop loin dans l'automatisation, car le Droit, en particulier le Droit contractuel, basé sur des principes immuables, tel que la bonne foi, la négociation, la proportion, requiert toujours l'intervention humaine[452].

Ainsi, si ces défis seront relevés, la *blockchain* pourrait réellement offrir une perspective prometteuse pour la sécurisation des données dans le contexte des connaissements électroniques et au-delà.

En outre, avec un développement sans cesse des technologies numériques dans le domaine maritime, la formation des marins et l'incitation à la recherche scientifique semblent être les piliers essentiels pour rester en phase avec les évolutions futures du secteur maritime.

Enfin, le devenir du marché de l'assurance cyber maritime ne saurait être parfaitement prédéterminé. Des lueurs d'espoir se dessinent et promettent un secteur plus résilient face à la cybercriminalité. Cependant, un long chemin reste à parfaire pour rattraper le retard et être en concordance avec l'évolution exponentielle des nouvelles technologies, Mais déjà, l'approche proactive qui s'est mise en place faciliterait dans le futur, l'adoption de mesures de défense adaptées aux risques cybernétiques.

[452] PIETTE G., Traité du Droit maritime, *op.cit.*, p.872.

CONCLUSION GÉNÉRALE

Trancher la question d'assurabilité du risque cyber en transport maritime n'est guère simple.

Alors que l'industrie maritime poursuit sa transformation numérique, l'assurance de la menace cyber deviendra un élément clé pour garantir la durabilité des opérations maritimes dans un environnement en constante évolution.

Par conséquent, les assureurs et les entreprises du secteur doivent collaborer étroitement pour comprendre les enjeux spécifiques à la cybersécurité maritime, développer des polices d'assurance adaptées et évaluer correctement les risques et les opportunités.

Néanmoins,*"se limiter à ne proposer que des solutions assurantielles serait une erreur*"[453].

Certes, les autorités publiques ont un rôle central en la matière[454], à savoir dans la mise en place d'un cadre juridique adapté ou encore dans la participation à la couverture assurantielle. Mais au-delà de l'apport des États, le développement d'une conscience cyber collective, plus solide, au sein des entreprises, revêt d'un intérêt essentiel pour la viabilité et la durabilité de cette industrie.

Tandis que le paysage des menaces évolue à un rythme effréné et gagne en complexité, les entreprises doivent admettre que la cybersécurité parfaite n'est plus qu'un mythe[455].

A présent, il n'est plus question de savoir si une cyberattaque arrivera mais de quand est-ce qu'elle arrivera et comment nous pouvons nous préparer à y faire face[456].

Tel que l'adage le résume, "*on ne récolte que ce que l'on sème"*. Si les différents acteurs maritimes auraient à instaurer une meilleure préparation aux

---

[453] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.78.
[454] TEHTRIS, *"Comment passer de la cybersécurité à la cyber résilience ?",* 30 juillet 2020, https://tehtris.com/ fr/ blog/ comment-passer-de-la-cybersecurite-a-la-cyber-resilience, Consulté le 28/08/2023.
[455] *Ibid.*
[456] CESAM, PARISMAT 2023, table ronde : *Comment l'écosystème maritime et aérien fait face à la montée du risque cyber ?*, *op.cit.*

incidents cybernétiques potentiels, la réponse, en cas de crise, serait plus rapide et efficace, ce qui réduirait, conséquemment, les pertes.

La stratégie à adopter serait donc fondée sur la cyber résilience. Il ne s'agit plus de se placer dans une position d'attente passive, mais de s'assurer que les affaires puissent suivre leur cours habituel en cas d'événement inattendu et de minimiser les dommages engendrés.

De simples gestes de résilience, tels que des mises à jour régulières des SI et un changement constant des mots de passe, pourraient faire la différence et échapper aux entreprises maritimes des pertes innombrables.

Tous les efforts de l'industrie doivent concourir à la construction d'une barrière efficace contre les risques *marétiques.*

Ainsi, *"la création d'un pool ou d'un club ne peut-elle pas résoudre le problème de capacité de l'assurance du cyberisque ?"*[457]

Pour conclure, comme l'a souligné Bernard IMPERIAL, directeur fondateur de CY Wake au PARISMAT 2023[458], il ne faut ni sous-évaluer ni surévaluer le risque cyber. Nous pouvons parfois avoir tendance à surestimer les pertes dans certains domaines et à les négliger dans d'autres.

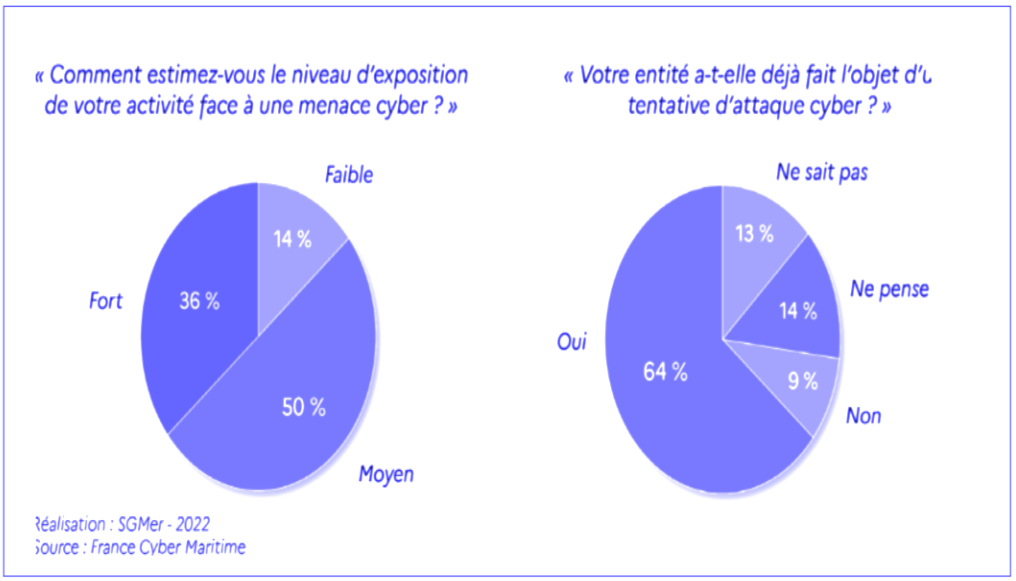
En réalité, la sensibilité du transport maritime varie en fonction du secteur. Ainsi, la situation des compagnies maritimes qui exploitent des navires à passagers se révélerait bien plus délicate en présence d'une menace cyber que celle des porte-conteneurs, et encore plus que celle des navires de pêche[459].

Dès lors, adopter une approche sectorielle de la réalité et trouver une solution assurantielle adéquate pour chaque situation, seraient les pièces maîtresses pour un avenir prospère et rayonnant du monde maritime des transports.

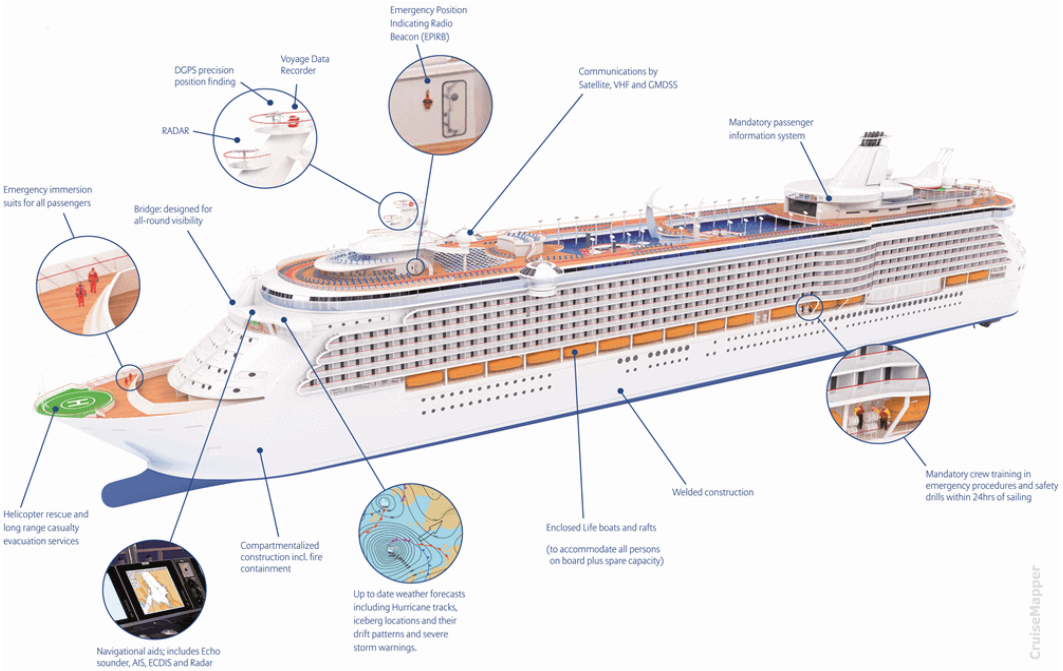
[457] LASMOLES O., *"Réflexions juridiques autour de l'assurance des cyber risques maritimes"*, *op.cit.*, p.78.
[458] CESAM, PARISMAT 2023, table ronde : *Comment l'écosystème maritime et aérien fait face à la montée du risque cyber ?*, *op.cit.*
[459] *Ibid.*

ANNEXES

Annexe 1 : La perception de la menace cyber par les acteurs du maritime (enquête publiée en juillet 2020), source : Cybersécurité maritime, l'économie bleue en France, éd. 2022, p.546.

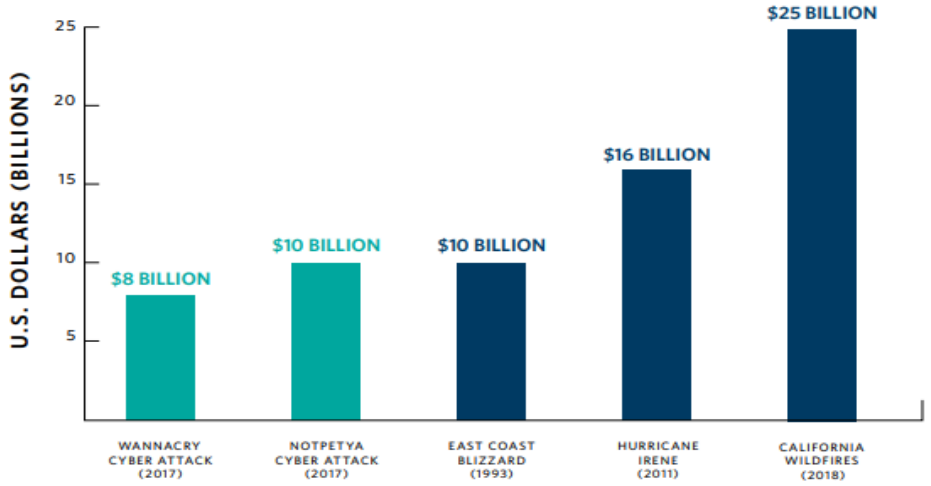


Annexe 2 : CruisMapper. Cruise Ship Safety. Available online: https://www. cruisemapper.com/wiki/751-cruise-ship-safety (accessed on 24/06/2023).



Annexe 3 : BATEMAN J., *"War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions"*, Carnegie Endowment for International Peace, p.7.

FIGURE 1
Global Cyber Attacks Compared With Select U.S. Natural Disasters

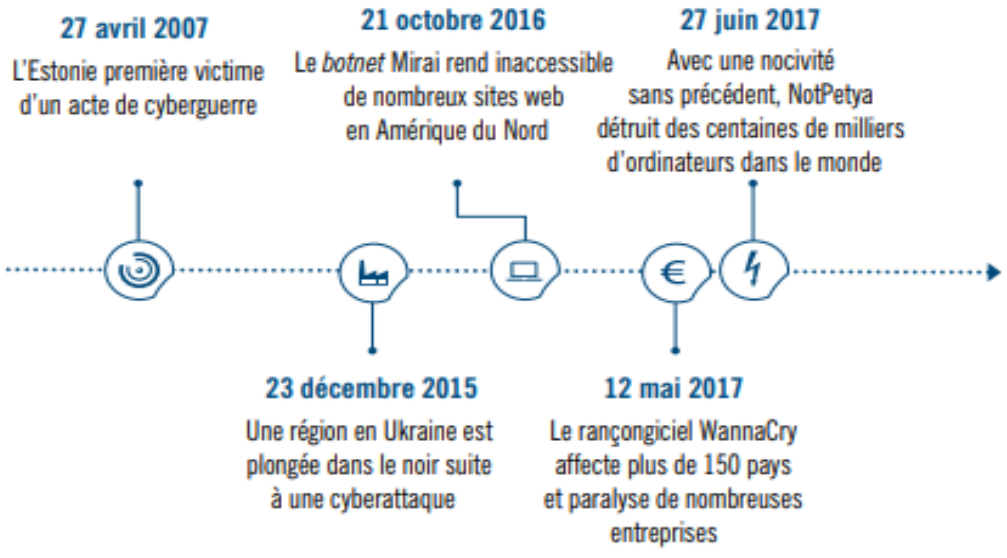


SOURCE: Luke Gallin, "Re/insurance to Take Minimal Share of $8 Billion WannaCry Economic Loss: A.M. Best," Reinsurance News, May 23, 2017, https://www.reinsurancene.ws/reinsurance-take-minimal-share-8-billion-wannacry-economic-loss-m-best/; PCS, "Could Not-Petya's Tail Be Growing?," 2019, https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf; and National Oceanic and Atmospheric Administration, "Billion-Dollar Weather and Climate Disasters: Events," 2020, https://www.ncdc.noaa.gov/billions/events.

NOTE: The cost of these U.S. disasters is calculated in 2020 dollars.

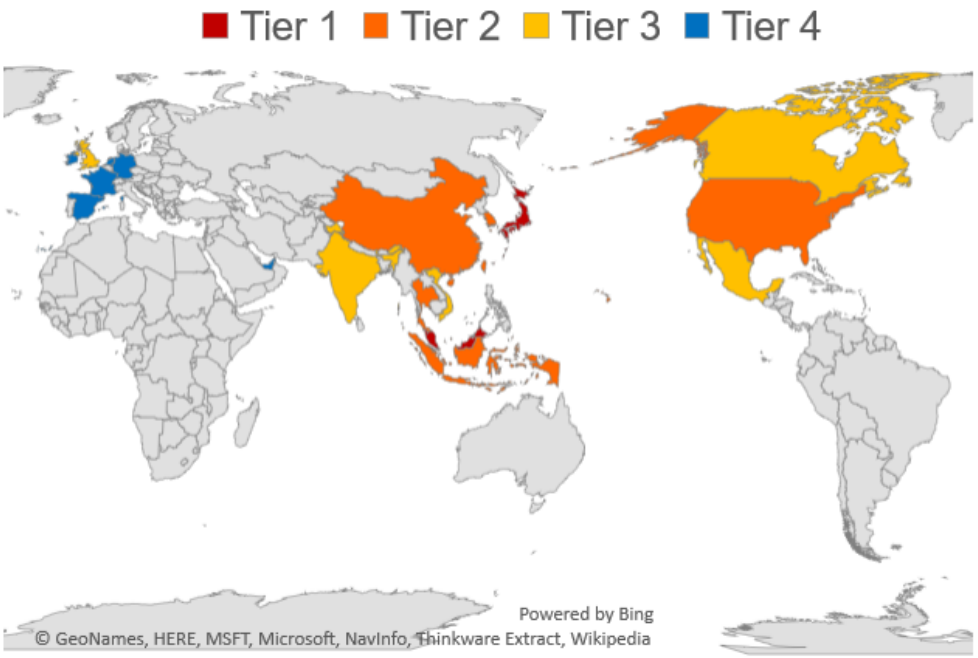
Annexe 4 : INSTITUT MONTAIGNE, *"Cybermenace : avis de tempête"*, novembre 2018, p.17.

Figure 1 – Quelques exemples marquants



27 avril 2007, l'Estonie première victime d'un acte de cyberguerre

Annexe 5 : CyRim report, *"Shen Attack: Cyber risk in Asia Pacific ports"*, 2019, https://assets.lloyds.com/assets/pdf-cyrim-shen-attack-final-report/1/pdf -cyrim -shen-attack-final-report.pdf, p.21.



Countries impacted are colour-coded to match the tier in the supply chain at which they are first impacted.

BIBLIOGRAPHIE

I- Ouvrages et Manuels

(Par ordre alphabétique des auteurs)

- DREYFUSS M.-L., La révolution digitale dans l'assurance, *éd.,* L'Argus de l'assurance : les fondamentaux, 2018, 332 pages.
- PIETTE G., Traité du Droit maritime, *éd.,* Pedone, 2023, 918 pages.
- TALEB N., The Black Swan: The Impact of the Highly Improbable, Random House, 2007, 400 pages.

II- Thèses, mémoires et études universitaires

(Par ordre alphabétique des auteurs)

- CHESNEAU A., *"Les "navires autonomes ". Enjeux et impacts d'une navigation sans équipage dans le monde maritime"*, HAL Open science, Droit, 22 janvier 2018, 93 pages.
- FEREY G., GROROD N., LEGUIL S., *"L'assurance des risques cyber"*, Sciences de l'Homme et Société, Mines Paristech, 2017, 77 pages.
- MATCHINDA O., *"La dématérialisation des documents de transport maritime de marchandises : (Étude dans le cadre de la CEMAC)",* Thèse de doctorat, Université Paris 1 Panthéon Sorbonne, 09 février 2021, 451 pages.
- THIAW I., *"L'assurance maritime face aux risques cybernétiques"*, Université de Lille, 2020, 126 pages.

III- Articles et revues

(Par ordre alphabétique des auteurs)

- AUBERGER C., *"Cybersécurité maritime, un enjeu stratégique pour tous les acteurs de la filière"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, pp. 7-13.

- BANITZ L., *"Les cyber risques dans le monde maritime : de la prise de conscience aux actes"*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, pp.23-27.
- BAUDU F., *"Les cyber-menaces contre les navires et les installations portuaires",* Gazette n°43, CAMP, 2017, pp.5-6.
- BELLAYER-ROILLE A., *"Entre souveraineté et transnationalité, les défis du droit de la mer",* Revue internationale et stratégique, 2014/3, n° 95, pp. 111-119.
- BENDER B., *"Un secteur uni pour faire face au risque cyber", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, pp.29-32.
- BENOTTI S., "*Piraterie maritime : la maîtrise du risque ?"*, ISEMAR, Note de synthèse, n° 199, avril 2018, 4 pages.
- COUSTILLERE A.,*"Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ?"*, RDNA, n°789, 2016/4, pp.44-48.
- FRONCZAK S., *"Lutte contre la cybercriminalité maritime : Prévôts de la mer contre pirates", in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, pp.45-53.
- GIBBS J., "*Cyber Risks and Insurance in the marine Industry"*, *in.*, Zelle LLP Insurance Law360, March 14th, 2016, 5 pages.
- HEON S., PARSOIRE D., "*La couverture du cyber-risque"*, Revue d'Economie Financière, n° 126, 2017/2, pp.169-182.
- IUMI, *"Insuring cyber risk"*, *in.,* Ship & offshore, n°5, 2017, pp.42-43.
- JACKSON S., *"Cyber 'war': a question of 'reasonable expectations",* Clyde&Co, IUMI EYE Newsletter, Mars 2022, n°36, p.11.
- JACQ O., *"Les perspectives en matière de réglementation et de bonnes pratiques en cybersécurité maritime"*, DMF, n°842, 1er janvier 2022 , 3 pages.
- KAO M.-B., *"Cybersecurity in the Shipping Industry and English Marine Insurance Law"*, Tulane Maritime Law Journal, vol. 45, no. 3, summer 2021, pp. 467-508.
- KEGELS A., *" Le transport autonome sur les voies navigables intérieures",* DMF, n°829, 1er novembre 2020, 4 pages.

- KERMARREC Y., *“ Cybersécurité et monde maritime : contexte, enjeux, challenges et opportunités”,* DMF, nº 842, 1er janvier 2022, 5 pages.
- LASMOLES O.,
    - *“Cybersécurité et navires sans équipage”*, DMF, n°817, octobre 2019, pp.771-782.
    - *“Réflexions juridiques autour de l'assurance des cyber risques maritimes”, in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, pp.69-78.
- LOOTGIETER S.,
    - *“Cyber-sécurité et Transport maritime”,* Gazette n°43, CAMP, 2017, pp.3-4.
    - *“Les risques cybernétiques dans le domaine des transports”* , DMF n° 775, 8 décembre 2015, 7 pages.
- MANET F.-C., “*La marétique, un enjeu essentiel pour l’humanité ?”*, *in.,* Cybersécurité maritime : Regards croisés, Cybercercle collection, 2020, p. 79-92.
- MOREL C., “*L’océan : un espace numérique convoité ? Des mers de câbles”*, *éd.,* Institut Français des relations internationales, RAMSES, 2019, p.46-51.
- PERRA F., *“ Les principes de l’assurance du risque cyber pour les compagnies maritimes”*, DMF n°842, 01 janvier 2022, 4 pages.
- PIETTE G., *“La sécurité en droit maritime à l’épreuve des nouvelles technologies”*, *in.,*Transport et sécurité, LexisNexis, 2019, pp. 317-330.
- QUASHIE F., ROLLAND E., SPINEC A., VALERO C., *“L’assurance maritime: évolution de la perception du risque”*, note de synthèse n° 192, ISEMAR, septembre 2017, 4 pages.
- VALERO C., TOURRET P., *“ 20 ans d'apports des technologies aux industries maritimes”*, Note de synthèse n°191, ISEMAR, Juin 2017, 4 pages.

IV- Réglementations et textes officiels

(Par ordre chronologique d'adoption)

A- Droit interne :

- Textes juridiques obligatoires :

- 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, JORF, 25 mai 2018, p. 1.
- Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772, Consulté le 05/08/2023.
- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. V. https://www.legifrance. gouv.fr/ jorf/article_jo/JORFARTI00002833890,
- Code des transports, en vigueur depuis le 1er décembre 2010, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000023086525, Articles, L5000-2-1, L5422-1.
- Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, JORF, 24 mai 2006.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004.
- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62 du 14 mars 2000.
- Arrêté du 23 novembre 1987 relatif à la sécurité des navires et à la prévention de la pollution, https://www.legifrance.gouv.fr/loda/ id/JORFTEXT 000000841523, Article 130.39.
- Code civil français, entré en vigueur depuis le 21 mars 1804, modifié par l'ordonnance n°2016-131 du 10 février 2016, Article 1242.

- Textes officiels non obligatoires :

- Ministère de l'économie des finances et de la souveraineté industrielle et numérique, Fiches pratiques, *"Assurance"*, Direction générale de la concurrence, de la consommation et de la répression des fraudes, 04 Août 2023.
- Avis, Conseil économique, social et environnemental, *"Climat, cyber, pandémie : le modèle assurantiel français mis au défi des risques systémiques",* JORF, avril 2022.
- Le Gouvernement Français, Secrétariat Général de la Mer, *"Cybersécurité maritime",* L'économie bleue en France, *éd.*, 2022, pp. 543-571.
- Banque de France, *"Une mesure de l'évolution du risque cyber"*, Billet n°246, 17 décembre 2021.
- Rapport d'information du Sénat français relatif à la cybersécurité des entreprises, n°678, 10 juin 2021.
- Assemblée Nationale, Rapport de la mission d'information commune sur la blockchain (chaîne de blocs) et ses usages : un enjeu de souveraineté, décembre 2018, 6 pages.
- Secrétariat Général de la Défense et de la Sécurité Nationale, instruction interministérielle relative à l'organisation et à la coordination de la sûreté maritime et portuaire, 27 juin 2018, Instruction n° 230/ SGDSN/PSN/NP.
- Guide Direction des Affaires Maritimes, Cyber sécurité- renforcer la protection des systèmes industriels du navire, janvier 2017. https://goo.gl/yv5EN9,
- Guide Direction des Affaires Maritimes, *"Cybersécurité évaluer et protéger le navire"*, septembre 2016.
- Guide des bonnes pratiques de sécurité informatique à bord des navires, L'ANSSI, mars 2015, https://goo.gl/ kS p rgG.

B- Droit communautaire :

- NIS 2, Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, https:/ /eur-lex.europa.eu/legal-content/FR/TXT
- Recommandation du comité Européen du risque systémique, Sur un cadre paneuropéen de coordination des cyber incidents systémiques pour les autorités concernées, (CERS/2021/17), 02 décembre 2021,
- Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.
- Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE), no 526/2013.
- Résolution du Parlement Européen contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)), 16 février 2017.
- 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.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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), https://eur-lex. europa.eu/legal -content/FR/TXT.

C- Droit international et comparé:

- BIMCO, Guidelines on cybersecurity on board ships, version 4, 2020, https://www.bimco.org/about-us-and-our-members/publications /the-guidelines - on-cyber-security-onboard-ships.
- OMI, Résolution MSC.428(98), sur la Gestion des Cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité (SGS), adoptée le 16 juin 2017, entrée en vigueur le 1er janvier 2021, https://wwwcdn.imo.org /localresources/fr/ OurWork/Security /Documents/MSC%20 98-23-Add.1.pdf.
- IMO, Guidelines on cyber risk management, 2017, https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/ MSC-FAL.1-Circ.3-Rev.1% 20-%20Guidelines%20 On% 20 Maritime % 20 Cyber%20Risk%20Management%20(Secretariat).pdf.
- ONU, Convention des Nations Unies sur le contrat de transport international de marchandises effectué entièrement ou partiellement par mer, Règles de Rotterdam, New York, 11 décembre 2008, https://uncitral.un.org/sites/uncitral .un.org/ files/media-documents/ uncitral/fr/ rotterdam - rules-f.pdf.
- Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23.XI.2001, entré en vigueur 1er juillet 2004, Série des traités européens - n°185, https://rm.coe.int/168008156d.
- The Computer Misuse Act of 1990, https://www.legislation.gov.uk /ukpga/1990/18/contents.
- ONU, Convention des Nations unies sur le droit de la mer (CNUDM), Montego Bay, 10 décembre 1982, entrée en vigueur le 16 novembre 1994, No 31363, https://treaties.un.org/doc/Publication/MTDSG/Volume%20II/Chapter %20XXI/XXI-6.fr.pdf, Article 101.
- Convention internationale pour l'unification de certaines règles en matière de connaissement, Conclue à Bruxelles le 25 août 1924, modifiée par le protocole du 23 février 1968 et par le protocole du 21 décembre 1979.
- OMI, Convention Internationale pour la sauvegarde de la vie humaine en mer (SOLAS), signée à Londres le 20 janvier 1914, http://archive.org/details/textofconvention00inte/page/n5/mode/2up?view= theater.

- OMI, chapitre XI-2 de la Convention SOLAS, CODE ISPS, Code international pour la sûreté des navires et des installations portuaires (ISPS), entré en vigueur le 1er juillet 2004.
- OMI, chapitre IX dans la Convention SOLAS, CODE ISM, Code international de gestion de la sécurité (Code ISM), résolution A.741(18), entré en vigueur le 1er juillet 1998.

V- Rapports

(Par ordre alphabétique des auteurs)

- ADAM Assurances, *"Les menaces cyber dans le secteur maritime: a-t-on déjà envisagé tous les scénarios ?*", Le Lab – Recherches et innovations en assurances maritimes et transport, 20 avril 2020, 4 pages.
- ADAM Assurances, *"Entre le risque cyber et le risque de guerre, où se trouve la frontière ?"* Le Lab, 22 octobre 2019, https://f.hypotheses.org/wp-content /blogs.dir/4944/files /2019/10/T %C3%A9l%C3%A9charger-4.pdf, 5 pages.
- ALLIANZ Global Corporate & Specialty,*"Cyber: The changing threat landscape Risk trends, responses and the outlook for insurance"*, 2022, 28 pages.
- BATEMAN J., *"War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*", Carnegie Endowment for International Peace, 72 pages.
- CHUBB N., FINN P., NG D., *" The great disconnect : The state of cyber risk management in the maritime industry "*, Thetius, Cyberowl, et HFW, 2022, 44 pages.
- CLUSTER MARITIME FRANÇAIS, Livre bleu sur la marétique, 2013, 58 pages.
- FEDEX, FedEx Corporation Annual Report, 2019, 162 pages.
- HOLMAN FENWICK WILLAN, *"Cyber risk adaptability and responsibility"*, December 2020, 4 pages.

- INSTITUT MONTAIGNE, *"Cybermenace : avis de tempête"*, novembre 2018, 107 pages.
- LE CLUB DES JURISTES, "*Rapport : Assurer le risque cyber"*, Tome 1, Janvier 2018, 25 pages.
- LEPETIT J.-F., "*Rapport sur le risque systémique"*, Ministère de l'Economie, de l'Industrie et de l'emploi, avril 2010, 103 pages.
- MARITIME MUTUAL, *"Defective passage plans and unseaworthiness : english supreme court decision in the CMA CGM Libra grounding case",* Maritime Mutual Risk Bulletin No. 53, 11 January, 2022, https://maritime-mutual.com/risk-bulletins/defective-passage-plans-and -unseaworthiness, 9 pages.
- OECD, *"Enhancing the Role of Insurance in Cyber Risk Management"*, OECD Publishing, 2017, Paris, 138 pages.
- THE AMERICAN CLUB, ABS GROUP, *"Managing cyber risks and the role of the P&I club : an overview",* october 2020, 14 pages.
- United States Government Accountability Office, Report on CYBER INSURANCE : *"Insurers and Policyholders Face Challenges in an Evolving Market"*, May 2021, 21 pages.
- VERIZON, *"Data breach digest report : Scenarios from the field"*, 2016, https://maritimecyprus.com/wp-content/uploads/2016/03/verizondata-breach-digest_en-1.pdf., 56 pages.

VI- Jurisprudence

- Affaire de la Royal Courts of Justice Strand, *MSC Mediterranean Shipping Company S.A vs Glencore International AG*, London, WC2A 2LL, 24/05/2017, https://www .quadrantchambers.com/.
- Affaire *McFadden v. Blue Star Line*, King's Bench division, 16/03/1905, 1 K.B, 697, *Cf.,* Case summary, https://lawfaculty.in/mcfadden-v-blue-star-line-kings-bench-division-16-march-1905-1905-1-k-b-697-channell-j.

VII- Articles de Presse

(Par ordre alphabétique)

- Cybernews, *"Opinion : Kaseya has dealt with cyberattack better than SolarWinds"*, publié le 28 septembre 2021, https://cybernews.com/security/ opinion -kaseya-has-dealt- with -cyberattack -better -than- solarwinds/.
- Financial Times, *"Insurers must rethink handling of cyber attacks on states"*, publié le 29 août 2022.
- Le Marin, *"Des terminaux pétroliers victimes d'une cyberattaque en Europe du nord"*, publié le 03 février 2022, https://lemarin.ouest-france.fr/ secteurs -activites/shipping.
- Le Monde, *" La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques"*, publié le 12 février 2023, https://www.lemonde.fr /economie/ article/ 2023/02/12/ la-guerre-en- ukraine-fait- basculer-le -monde-dans -l-ere- des - cyberattaques.
- Lloyd's List, *"Shipping is 'decades behind' on cyber security, KPMG warns"*, publié le 6 mai 2014.
- Lloyds list, OSLER D, *"One ship is hacked everyday on average"*, publié le 06 juillet 2021.
- Palmer, ZDNet, *" Security researchers spot another form of wiper malware that was used against Ukraine's networks",* 2022.
- Seatrade Maritime News, *" Cyber-attack allows pirates to target cargo to steal",* 07 juillet 2016, https:// www. seatrade - maritime. com/ americas /cyber-attack-allows-pirates-target-cargo-steal.
- The Maritime Executive, *"Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data"*, publié le 26 novembre 2021, https://maritime-executive.com/article/ransomware-attack-on-swire-pacific-off shore.
- The New York Times, *"Cyberattack Forces a Shutdown of a Top U.S. Pipeline",*publié le 08 mai 2021, https://www.nytimes.com/2021/05/08/ us/ politics/ cyberattack-colonial-pipeline.
- Tradewinds, *" Sophisticated scams highlight growing cyber risk to shipping"*, publié le 10 octobre 2014.

VIII- Lexique et dictionnaires

- BRAUDO S., Dictionnaire du Droit privé, *https://www.dictionnaire-juridique.com/.*
- Cambridge dictionary, *https://dictionary.cambridge.org/.*

IX- Sites internet

(Par ordre alphabétique)

- ANSSI,
  - *"Directive NIS 2 : Ce qui va changer pour les entreprises et les administrations françaises"*, publié le 17 janvier 2023, https://www.ssi.gouv.fr/directive-nis-2-ce-qui-va-changer-pour-les-entreprises-et-ladministration-francaises/.
  - *"Un niveau élevé de cybermenaces en 2022",* publié le 24 janvier 2023,https://www.ssi.gouv.fr/actualite/un-niveau-eleve-de-cybermenaces -en-2022/.
- Archimer, IFREMER, https://archimer.ifremer.fr/.
- Astaara Co. Limited, *"LMA 5403, a lost opportunity ?"*, juillet 2020, https://astaaragroup.com/wp-content/uploads/2020/07/LMA-5403-A-Lost-Opportunity.pdf ,
- Axa insurance-reinsurance website,"*The LockerGoga Ransomware Attack: A worst-case scenario for industrial operations"*, publié le 03 juin 2019, https://axaxl.com/fast-fast-forward/articles /the -lockergoga- ransomware -attack_a-worst-case-scenario-for-industrial-operations.
- BAUME T., " *Cyber - risques : les difficultés des assureurs pour apporter la bonne réponse",* L'Argus de l'assurance, 25 juin 2014, https://www.argusdelassurance.com/risk-management/cyber-risques-les-difficultes -des-assureurs-pour-apporter-la-bonne-reponse.79683
- BREWER J., "*Marine Insurance Market is Sharpening its Focus on Cyber Attack Risk."*, ALL ABOUT SHIPPING.Co.UK, May 25, 2015, www.allaboutshipping.co.uk/2015/05/25/marine-insurance-market-is-sharpening-its-focus-on-cyber-attack-risk/.
- CentralEyes, *"The Top Cybersecurity Breaches in the UAE"*, May 16th 2022, https://www.central eye.com/ the-top-cybersecurity-breaches-in-the-uae/.

- CESAM (Comité d'études et de services des assureurs maritimes et transports), https://www.cesam.org/.
- CHUBB , *"Cyber Systemic Risk/Product Update: broker FAQs",* https ://www.chubb.com/content/dam/chubb-sites/chubb-com/fr-fr/campagne-digitale/cyber/ FAQ- courtiers-risques.
- CIO Letter, *"Cyber, de la sécurité à la résilience",* mai 2022, p.2. https://alternativeviews.tikehaucapital.com/sites/tikehau-cap-blog/files/CIO% 20 Letter /CIO-Letter-FR.pdf.
- CMI, Rules for electronic bills of lading, juin 1990, https://comitemaritime.org/work/rules- for-electronic- billing-of-lading/,
- CNIL, Commission nationale de l'informatique et des libertés, site officiel,
  - https://www.cnil.fr/fr/definition/ blockchain,
  - https://www.cnil.fr/fr/definition /cloud-computing,
- Cyber Malveillance, https://www. cybermalveillance. gouv.fr/.
- Cybercrime in shipping, https://comitemaritime.org/work/cybercrime/.
- DIONE A., *"L'assurabilité du connaissement électronique dans le cadre du transport maritime de marchandise"*, Actualité juridique du village de la justice, https://www.village-justice.com/articles/.
- Docs du juriste, Commentaire *"Sociologie Juridique, chapitre 1 - Jean Carbonnier (1978) - La sociologie juridique avant le XXe siècle"*, https:// www.doc-du-juriste.com/droit-prive-et-contrat/droit-civil/commentaire-de-texte/sociologie-juridique-chapitre-1-jean-carbonnier-1978-sociologie-juridique-avant-siecle.
- GREENWALD J., *" Silent cyber ruling has insurers looking closer at war clause",* Business Insurance, Risk Management, March 04th, 2022, https://www.businessinsurance.com/article/20220304/NEWS06/912348162/ Silent-cyber-ruling-has-insurers-looking -closer -at-war-clause
- IBM,
  - *"Pourquoi les menaces internes sont-elles particulièrement dangereuses"*, https://www.ibm.com/ fr-fr/topics/insider-threats.
  - *"Présentation client de la plateforme TradeLens",* 17 avril 2019, https://www.ibm.com/downloads /cas /XNGVO4AY.
  - "*Qu'est ce qu'une cyberattaque ?",* https://www.ibm.com/fr-fr/ topics/cyber-attack/.

- Lloyds, *"Shen Attack: Cyber risk in Asia Pacific ports"*, publié le 14 octobre 2019, https://www.lloyds.com/news-and- insights/ risk-reports / library/shen-attack-cyber-risk-in-asia-pacific-ports.
- Ministère de l'économie des finances et de la souveraineté industrielle et numérique, *"Qu'est ce qu'une chaîne de blocs (blockchain) ?",* Bercy Info, 12 avril 2022, https://www.economie.gouv.fr/entreprises/blockchain -definition -avantage- utilisation- application.
- Northbridge Assurances, *"Qu'est-ce-qu'un cyber risque ?"*, https://www.nbins.com/fr/blog/ cyberrisques /qu-est-ce-qu-uncyberrisque.
- OMI, site officiel, https://www.imo.org/fr/OurWork/Security/Pages/ Cyber-security.aspx,
- REMY M., "*La blockchain au service de l'assurance maritime"*, L'Argus de l'Assurance, 08 novembre 2018, https://www.argusde lassurance.com/tech/la-blockchain-au-service-de-l-assurance-maritime.136654
- Seatrackbox, https://www.seatrackbox.com/.
- TEHTRIS, *"Comment passer de la cybersécurité à la cyber résilience ?",* 30 juillet 2020, https://tehtris.com/fr/blog/comment-passer-de-la-cybersecurite -a-la-cyber-resilience.
- WTW, HILL A., *"Silent Cyber: ce que vous devez savoir"*, 07 juin 2021, https://www.wtwco.com/fr-ch/insights/2021/01/silent-cyber-what-you-need-to-know.

X-Conférences

- CESAM, PARISMAT 2023, table ronde : *"Comment l'écosystème maritime et aérien fait face à la montée du risque cyber ?*", 27 juin 2023, intervention disponible sur : https://www.youtube.com/watch?v=vIEMA eHusno.

XI- Polices et clauses d'assurance

(Par ordre chronologique d'adoption)

- Marine Cyber Exclusion endorsement Clause (LMA5402), Lloyd's Market Association, november 11th 2019, https://www.lma lloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031 PD.aspx.
- BIMCO, Cyber Security Clause 2019, https://www.bimco.org/ contracts-and-clauses/bimco-clauses/current/cyber- security-clause-2019,
- Conventions spéciales RG WB 2018 pour l'assurance des facultés (marchandises) transportées par voie maritime contre les risques de guerre, de terrorisme et de grève, Garantie Waterborne du 1er juillet 2018, Article 2.
- CL 380, Allianz Institute Cyber Attack exclusion clause, november 10th 2003, https://www.allianz.com.tr/content/dam/onemarketing/aztr/allianz/ pdf/ diger/Tekne-Kloz-Metinleri-04022020.pdf.

TABLE DES MATIÈRES

4ème de couverture

Résumé du mémoire (rédigé dans la langue originale du mémoire / 500 mots max)

Dans un monde maritime de plus en plus connecté et numérisé, le risque cyber évolue pour devenir l'une des principales menaces auxquelles les entreprises maritimes sont confrontées. Ces attaques peuvent perturber les opérations maritimes, compromettre la sécurité des navires, des cargaisons et des infrastructures portuaires, et engendrer même des risques environnementaux.

Face à l'évolution de ce risque et la multiplication des attaques cybernétiques, l'industrie maritime commence sérieusement à repenser sa manière d'agir face à ces menaces. D'emblée réticente et inconsciente des lourdes pertes et dommages que ce risque peut entraîner, l'industrie maritime commence, à présent, à adopter une stratégie préventive dans le but de sécuriser ces opérations.

L'assurance de ce risque demeure, néanmoins, essentielle. La nature particulière de la menace cyber et sa nouveauté semblent contribuer à la multiplication des attaques et des dommages qu'ils en résultent. Le risque zéro n'existant jamais, on s'interroge ainsi sur l'assurabilité de cette menace.

Ce mémoire, nous offre un aperçu essentiel des obstacles que doivent surmonter les assureurs et les entreprises maritimes. En fin de compte, ce travail propose les bases d'une approche plus solide et complète pour aborder les défis complexes de l'assurabilité des risques cyber dans le secteur du transport maritime, tout en assurant la résilience et la pérennité de cette industrie vitale.

Mots-clés définis par l'auteur ou autrice (3 à 5 mots-clés) :

- Risque cyber
- Assurances maritimes
- Transport maritime
- Cybersécurité