UNIVERSITE D'AIX-MARSEILLE

FACULTE DE DROIT ET SCIENCES POLITIQUES

POLE TRANSPORTS CENTRE DE DROIT MARITIME ET DES TRANSPORTS

PROTECTION CONTRE LA CYBERCRIMINALITE

DANS L'INDUSTRIE MARITIME

MEMOIRE POUR L'OBTENTION DU MASTER 2 DROIT ET MANAGEMENT DES ACTIVITES MARITIMES

DAVID YUNUS BANSARD

SOUS LA DIRECTION DE MONSIEUR LE PROFESSEUR CYRIL BLOCH,

ET DE MAITRE CHRISTOPHE THELCIDE,

2019/2020

UNIVERSITE D'AIX-MARSEILLE

FACULTE DE DROIT ET SCIENCES POLITIQUES

POLE TRANSPORTS CENTRE DE DROIT MARITIME ET DES TRANSPORTS

PROTECTION CONTRE LA CYBERCRIMINALITE

DANS L'INDUSTRIE MARITIME

MEMOIRE POUR L'OBTENTION DU MASTER 2 DROIT ET MANAGEMENT DES ACTIVITES MARITIMES

DAVID YUNUS BANSARD

SOUS LA DIRECTION DE MONSIEUR LE PROFESSEUR CYRIL BLOCH,

ET DE MAITRE CHRISTOPHE THELCIDE,

2019/2020

REMERCIEMENTS

A ma mère et à mon père pour leur soutien et leur force sans faille

A Maître Christophe Thelcide pour sa rigueur, sa patience et sa disponibilité

A Monsieur le Professeur Cyril Bloch pour la pertinence de ses enseignements et l'opportunité donnée

A Monsieur Paul Franquart pour sa patience et le partage de son expertise

A Monsieur Fabien Caparros pour sa disponibilité et le don de son savoir

A Monsieur Antoine Person pour sa disponibilité et la qualité de ses conseils

A Monsieur Bruno Bender pour sa disponibilité et la profondeur de ses vues

A Maître Henri Najjar pour sa disponibilité et la pertinence de sa parole

A Monsieur Boris Fédorovsky pour sa générosité

A Monsieur Laurent Fedi pour ses conseils

A Monsieur Michel Botalla-Gambetta pour ses orientations

A Monsieur Jean Baptiste Salaün pour son aide

A Monsieur Igor Savostianoff pour son aide

LISTES DES ABRÉVIATIONS

AIS	Automated Identification System
CSIRT	Computer Security Incident Response Team
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ECDIS	Electronic Chart Display and Information System
FSN	Fournisseur de Service Numérique
GPS	Global Positioning System
ISM	International Safety Management
ISO	International Organization for Standardisation
OSE	Opérateurs de Services Essentiels

SOMMAIRE

Introduction

« *Les hommes n'acceptent le changement que dans la nécessité et ils ne voient la nécessité que dans la crise* ». Jean Monnet

1. Le développement des systèmes d'information a semblé comme une promesse de facilité, de confiance et d'efficacité dans de nombreux domaines, y compris dans le domaine maritime. Le terme même de cybernétique, qui a trait à l'étude des systèmes d'informations complexes, n'a-t-il pas pour origine le vocable grec *kubernetes,* qui désigne le pilote ?

2. Cependant, ce développement des systèmes d'information s'est également accompagné de menaces. Ces systèmes ont en effet permis l'émergence d'une nouvelle criminalité appelée cybercriminalité. Ce terme désigne « l'ensemble des infractions pénales commises sur les réseaux de communications, en particulier Internet ».[1] Cette définition générale englobe effectivement les attaques subies par les différents acteurs de l'industrie maritime. La cybercriminalité comprend en son sein la réalisation de cyber-attaques, qui se définit comme une atteinte à des systèmes informatiques réalisée dans un but malveillant[2].

[1] *www.larousse.fr* [en ligne]. Disponible à l'adresse : https://www.larousse.fr/dictionnaires/francais/cybercriminalit%C3%A9/10910062

[2] RISQUES Prévention des risques majeurs. [en ligne]. Disponible à l'adresse : https://www.gouvernement.fr/risques/risques-cyber

3. Le terme de cybercriminalité, quant à lui, renvoie à l'accomplissement d'actes illicites par voie informatique à la poursuite d'un intérêt principalement économique. Seul ce type d'attaques sera analysé car il constitue la motivation première des deux attaques ayant le plus impacté l'industrie maritime. Il s'agit de celle subie par le port d'Anvers en 2011, puis de celle lancée contre les systèmes informatiques de l'armateur danois Maersk.

4. Par conséquent, les problématiques liées au cyberterrorisme ou au cyber-espionnage ne seront pas prises en compte dans le cadre de ce mémoire.

5. Ces attaques seront réalisées dans le cyberespace, qui est un espace où plusieurs équipements sont interconnectés.

6. Pour se protéger face à ces différentes attaques, la prise en compte de la cybersécurité sera primordiale. Celle-ci se définit comme « l'état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent où qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité que les systèmes offrent ou qu'ils rendent accessibles »[3].

7. Ensuite, le terme de protection sera pris dans une acception restreinte. En effet, le National Institute of Standards and Technology américain définit la cybersécurité par la mise en place de cinq étapes. La protection efficace d'un système d'information passe par l'identification, la protection, la détection, la défense et le rétablissement du système.

[3] Glossaire. *www.ssi.gouv.fr* [en ligne]. Disponible à l'adresse : https://www.ssi.gouv.fr/entreprise/glossaire/c/

8. L’identification consiste en la qualification des rôles et responsabilités du personnel pour la gestion du cyber et l’identification des systèmes, biens, données et capacités qui, lorsqu'ils sont perturbés, posent un risque aux opérations du navire.

9. La protection, quant à elle, suppose une mise en place de processus et de mesures relatives au contrôle du risque, et l’établissement de plans d’urgence afin de défendre un système contre un incident cyber, afin de garantir la continuité des opérations.

10. Ainsi, l’on peut voir que selon cette acception, une protection efficace d’un système d’information suppose que l’attaque ne se réalise pas. Dès lors seuls les éléments nécessaires à l’identification et à la protection seront abordés dans le cadre de ce mémoire.

11. Par conséquent, les éventuelles sanctions liées à la protection des données, telles que prévues par le Règlement n° 2016/679 sur la protection des données, ne seront pas prises en compte car elles supposent la réalisation d’une attaque informatique.

12. De surcroît, d’un point de vue pratique, la majeure partie des problèmes affrontés dans le cadre de la cybersécurité concerne ces deux aspects.

13. On prendra en considération, comme acteurs de l’industrie maritime, les autorités portuaires ainsi que les armateurs de navires marchands. Cependant, certaines perspectives dans le sens d’une amélioration de la cybersécurité offerte par les navires de service seront également tracées.

14. Enfin, le cadre du mémoire sera circonscrit aux exemples européens et français.

15. En effet, si une pléthore de documents traite des exemples américains ou étrangers de gestion de la cybersécurité par les différents acteurs maritimes, l’expérience de

terrain, les témoignages de première main nous semblent primordiaux pour un raisonnement pragmatique au regard des enjeux.

16. A ce titre, les personnes suivantes ont bien voulu accorder leur témoignage et faire part de leur expertise :

17. Monsieur Paul Franquart, Autorité Qualifiée en Sécurité des Systèmes d'Information au Grand Port Maritime de Marseille.

18. Monsieur Fabien Caparros, Chef de la Division chargé des Méthodes de Management et de la Sécurité Numérique à l'Agence Nationale de la Sécurité des Systèmes d'Information.

19. Monsieur Antoine Person, Secrétaire Général au sein de Louis Dreyfus Armateur.

20. Monsieur Bruno Bender, Coordinateur Cybersécurité Maritime pour le Comité France Maritime, rattaché au Secrétariat Général de la Mer.

21. Maître Henri Najjar, Avocat au Barreau de Paris.

22. Le sujet est traité dans le contexte d'une automatisation et d'une digitalisation toujours plus poussées de l'industrie maritime.

23. A ce titre, de nouvelles compagnies maritimes spécialisées dans les navires autonomes, tels que Massterly, voient le jour. Rolls-Royce a en outre testé un ferry autonome dans l'archipel de Turku en Finlande. Enfin, l'Organisation Maritime

Internationale a également mis en place le 14 juin 2019 des lignes directrices intérimaires pour l'essai de navires autonomes[4].

24. En effet, l'automatisation des navires a pour avantage principal d'éliminer l'élément humain et les erreurs qui en découlent dans le cadre de la navigation maritime. Elle permet également d'économiser les coûts résultant de l'accommodation et du paiement des marins[5].

25. Cette réduction de coûts est manifeste dans l'utilisation de moteurs intelligents, dont la consommation de carburant optimisée fait le succès parmi les armateurs.

26. Cependant, ces nouveaux outils qui apportent des solutions suscitent eux-mêmes des risques si leur sécurisation n'est pas effectuée par leur concepteur ou leur utilisateur. Par ailleurs les entreprises de l'industrie maritime sont de plus en plus soumises à une exigence de sécurité des données de leurs clients.

27. A ce titre, la responsabilité d'un acteur de l'industrie maritime est susceptible d'être engagée si les données communiquées par le client sont visées, attaquées, ou seulement non protégées par l'armateur ou l'autorité portuaire.

28. En ce sens le règlement général sur la protection des données prévoit de lourdes sanctions en cas de pertes des données de l'utilisateur.

29. Le sujet abordé présente de multiples intérêts. Tout d'abord, résolument contemporain, il s'inscrit dans des problématiques fondamentales de la pratique du droit

[4] Organisation Maritime Internationale, *INTERIM GUIDELINES FOR MASS TRIALS* en ligne. 14 juin 2019.

[5] ATMATSIDIS, K. Autonomous ships and The Cyber Security Challenge. *Maritime Risk International.* 2 avril 2019, n°Avril 2019.

maritime. A ce titre, Maître Christian Scapel et M. le Professeur Pierre Bonassies relient la cybersécurité du navire à sa navigabilité[6].

30. Pour déterminer la navigabilité d'un navire une question doit se poser : est-ce que le navire bénéficiait au commencement du voyage d'un état de navigabilité dont un propriétaire prudent pourrait se contenter ?

31. Cette navigabilité peut être commerciale. Dans ce cas de figure, le navire doit être armé convenablement pour les opérations qu'il devra entreprendre.

32. De plus, cette navigabilité pourra également être technique. A ce titre, si la coque et les moteurs se caractérisent par cette navigabilité, les différents systèmes à bord devront également être contrôlés, selon certains praticiens. Le navire sera donc navigable si les systèmes d'information à bord du navire garantissent qu'il peut entreprendre le voyage de manière sécurisée. Par conséquent, si un navire subit un dommage alors même que des précautions liées à la cyber sécurité ne sont pas prises, il est tout à fait vraisemblable qu'il ne sera pas considéré comme navigable. Les conséquences contractuelles, notamment liées aux couvertures, pourront dans ce cas de figure, être catastrophiques pour un armateur[7].

33. Par ailleurs, le sujet proposé s'inscrit comme nous allons le voir dans le cadre de la sécurité et la sûreté maritime.

34. S'agissant de la sécurité, différentes aides à la navigation rendues obligatoires telles que le GPS et l'ECDIS permettent de limiter les risques d'abordage. Aujourd'hui, ces

[6] BONASSIES, P., SCAPEL, C. *Traité de Droit Maritime.* LGDJ. Lextenso.p.605

[7] ROCHE, P. Safety Management, Due Diligence and Seaworthiness. *Maritime Risk International.* 21 avril 2018, vol. avril 2018.

systèmes sont constamment reliés aux satellites, ce qui les rend vulnérables à différentes attaques.

35. Après avoir évoqué les intérêts juridiques du sujet, il faut maintenant en venir à son intérêt économique.

36. Nous verrons que la mise en place d'une cybersécurité effective constitue bien trop souvent, pour certains acteurs de l'industrie maritime, un investissement à retour faible voire inexistant.

37. En effet, au vu de l'apparente rareté des attaques subies, l'engagement de ressources pour une protection contre un événement infiniment peu probable peut sembler superflu. Néanmoins les attaques réalisées ont un impact financier bien plus élevé que celui de la mise en place d'une cybersécurité. Par conséquent une évaluation du risque et une décision liée à celui-ci conditionneront l'ensemble des mesures prises ou non dans le sens d'une cybersécurité.

38. Enfin l'intérêt du sujet est de mettre en évidence la difficulté que peut présenter la mise en place des mesures de cybersécurité. Elles sont liées à la nature même du droit maritime, mais surtout à sa pratique. En effet, si l'on peut considérer que la France et les pays de l'Union Européenne disposent d'un droit maritime complet, l'application de ce dernier dans une situation impliquant un cocontractant d'un autre Etat peut très souvent se révéler compromise.

39. Par nature international, le droit maritime ne dispose pas d'un référentiel contraignant qui puisse s'appliquer à l'ensemble des acteurs prenant part à l'industrie maritime. Cette absence de régulation s'illustre par une concurrence exacerbée entre acteurs de même rôle. Elle se déploie sans régulation pour assurer à chaque compétiteur une disponibilité, une efficacité supérieure et des coûts inférieurs. Ainsi, chaque

nouvelle règlementation cherchant à s'imposer dans l'industrie maritime peut très vite être considérée comme une contrainte. Les problématiques de cybersécurité n'échappent pas à cette règle. Par ailleurs, si un acteur de l'industrie maritime se fait attaquer, il est grandement plausible que cette attaque ne soit pas signalée afin de ne pas mettre à mal l'image de l'acteur considéré.

40. Par conséquent, à moins que les nouvelles règlementations reflètent un besoin ou une prise de conscience exprimés par le marché, elles seront davantage perçues comme des difficultés qu'une sécurisation. Elles pourront donc être contournées. Dans le cadre de l'édiction de règles de droit positif, cet élément est absolument à prendre en compte. En effet, si les lois en matière de cybersécurité sont considérées trop contraignantes par les armateurs, le risque encouru sera notamment le dépavillonnement des navires.

41. Par ailleurs, chacun des acteurs de l'industrie maritime est confronté à des risques concrets, imminents, repérables, alors que le risque cyber apparaît lointain, peu compréhensible.

42. Enfin, l'industrie maritime est souvent considérée comme adoptant tardivement les nouvelles technologies[8]. Ce constat est d'autant plus valable, en termes de cybersécurité, comme en attestent plusieurs experts et institutions[9]. Nous subsumerons cet ensemble d'habitudes, d'intérêts, de comportements sous l'expression de facteur humain. Enfin, une autre difficulté ayant trait à la cybersécurité tient au fait qu'il n'existe pas de recette miracle ou de procédure à suivre à la lettre pour mettre en place un système qui permettrait l'élimination certaine de tout risque. D'un point de vue financier, une approche consistant à se prémunir dans l'ensemble des cas de figure d'attaques cyber dans chacune de leurs étapes serait tout simplement inaccessible vu

[8] FLOCKHART, F., HADWIN, S., MANSIGANI, R. Time to take Stock of Cyber Risk. *Maritime Risk International.* 14 octobre 2017, vol. Octobre 2017.

[9] OSLER, D. Shipping is "decades behind" on cyber security, KPMG warns. *Lloyd's List.* 6 mai 2014.

son coût. Ainsi la meilleure sécurisation d'un système d'information au regard des ressources disponibles restera bien souvent à la discrétion du responsable informatique d'une entreprise.

43. Dans ce cadre nous nous efforcerons de répondre à la question suivante : dans quelle mesure le facteur humain est-il l'obstacle principal à la mise en oeuvre d'une cybersécurité effective au bénéfice des agents de l'industrie maritime ?

44. L'on pourrait partir du constat de la défaillance de la cybersécurité dans l'industrie pour ensuite analyser en quoi s'imposent les dispositifs juridiques et techniques ayant trait à ce sujet. Cependant une certaine rigueur logique rend nécessaire de commencer par la suffisance du socle juridique et technique à disposition, puis de mettre à jour les insuffisances dans l'exécution des mesures préconisées des points de vue technique et juridique. En effet, elles constituent un environnement donné aux acteurs, auquel ils réagissent par la conformité ou la déviance. Il convient donc d'analyser dans une première partie la suffisance du socle juridique et technique actuellement en vigueur pour la protection contre la cybercriminalité dans l'industrie maritime, avant de rechercher les défaillances humaines dans l'exécution des dispositifs prévus.

PARTIE I LA SUFFISANCE DU SOCLE JURIDIQUE ET TECHNIQUE EN VIGUEUR POUR LA PROTECTION CONTRE LA CYBERCRIMINALITÉ DANS L'INDUSTRIE MARITIME

46. Selon Bruno Bender [10], la mise en place d'une cybersécurité efficace nécessite trois éléments. Tout d'abord, une base légale est nécessaire. En effet, elle habilite les organes étatiques à agir. Cette action ne sera pas entravée -du moins, a minima- par une quelconque action où un juge serait susceptible d'invalider les actions entreprises en raison de leur manque de légalité. Ensuite, il est nécessaire que les différents acteurs d'une même industrie utilisent la même sémantique, en d'autres termes, que ces acteurs parlent le même langage. Lorsque ces deux étapes sont mises à exécution, le troisième objectif est la coordination des différents acteurs.

47. Dans le présent titre, l'on procèdera en sens inverse, en envisageant d'abord la coordination. Cette approche obéit à un souci de réalisme. En effet, comme il a été affirmé dans l'introduction, l'industrie maritime se caractérise par une grande liberté en raison d'une concurrence exacerbée intrinsèque. Dès lors, ses modifications et ses mutations, selon Fabien Caparros, se font soit à raison d'une prise de conscience par l'industrie d'un problème considéré, soit par une règlementation nationale ou

[10] Coordinateur Cyber pour le Comité France Maritime.
Créé lors des Assises de la Rochelle le 8 Novembre 2016, le Comité France Maritime est codirigé par le Secrétariat Général à la Mer ainsi que le Président du Cluster Maritime Français, BENDER, B. [audio]. 26 juin 2020.

internationale[11]. Bien souvent, c'est la prise de conscience commune d'une industrie considérée qui est le moteur d'une évolution en termes de droit positif.

48. Dans la présente partie, il sera fait référence à un socle en vigueur. L'on entend par cette formule toute norme, de droit positif ou de droit souple, communément utilisée au sein de l'industrie maritime.

49. Sera analysée dans un premier temps la suffisance du socle en vigueur pour la coordination nécessaire des acteurs de l'industrie maritime afin d'optimiser leur cybersécurité (Titre I). Puis, dans une seconde partie, la suffisance du socle en vigueur pour la gestion organique et atomisée de la cybersécurité dans l'industrie maritime (Titre II).

[11] CAPARROS, F. [audio]. 2 juillet 2020.

TITRE I - LA SUFFISANCE DU SOCLE EN VIGUEUR POUR LA COORDINATION NÉCESSAIRE DES ACTEURS DE L’INDUSTRIE MARITIME POUR L’OPTIMISATION DE LEUR CYBERSÉCURITÉ

50. Cette coordination est nécessaire à plusieurs égards. Premièrement, l'industrie maritime n'a aucunement attendu la digitalisation pour procéder à la sécurisation de processus marqués par l'interaction de plusieurs entités. Cette imbrication s'est accentuée au fil des dernières années avec la multiplication des interfaces auxquelles sont soumis les différents acteurs de l'industrie. A titre d'exemple, le conteneur est en principe propriété de l'armateur, mais lors de son acheminement il transitera par un port, qui sera alors dans l'obligation de l'entreposer de manière sécurisée, et à ce titre de vérifier l'entreposage de l'ensemble des conteneurs. Finalement, ce conteneur aura son intégrité protégée par un cargo community system.

51. Deuxièmement, c'est précisément cette imbrication des entités qui rend la coordination nécessaire. En effet, aujourd'hui, l'anonymat classique d'un navire est quelque peu compromis, puisqu'il est en permanence relié à la terre par plusieurs logiciels tels que ceux relatifs à la navigation ou à la propulsion. Dès lors, les différents acteurs interconnectés forment des maillons de sécurité. L'objectif de l'attaquant sera donc de trouver le maillon le plus faible, et potentiellement d'impacter toute la chaîne formée.

52. Par conséquent, se construit aujourd'hui en France une coordination horizontale entre les différents acteurs de l'industrie maritime en matière de cybersécurité (Chapitre 1), ainsi qu'une coordination verticale grâce à l'établissement de référentiels communs (Chapitre 2).

CHAPITRE 1 - LA COORDINATION HORIZONTALE DES ACTEURS DE L'INDUSTRIE MARITIME

53. Cette coordination a été entérinée en 2018 par le Secrétariat Général à la mer et le Comité Interministériel de la Mer. En effet, ces deux institutions ont mis en chantier la création d'un Centre de Coordination de la Cybersécurité au profit de l'ensemble des acteurs de l'industrie maritime. Par ailleurs, le Conseil Cybersécurité du Monde Maritime (C2M2) a vu le jour en 2019. Ses travaux sont aujourd'hui notamment pilotés par le Secrétariat Général à la Mer et le Comité Interministériel de la Mer. Dans le champ de la cybersécurité maritime en cours d'élaboration, deux missions principales sont suivies, d'une part susciter une prise de conscience des acteurs de l'industrie maritime vis-à-vis des problématiques de sécurité, d'autre part préconiser de nouvelles démarches dans l'optique d'une optimisation de la cybersécurité. Il faut donc analyser dans un premier temps la prise en compte de la cybersécurité maritime dans le cadre de l'action de l'Etat en mer (Section I). Devront ensuite être évaluées les mesures préconisées (Section II).

Section I - L'inclusion de la cybersécurité maritime dans l'action de l'Etat en mer

54. Le décret n°95-1232 en date du 22 novembre 1995 instaure deux entités, le Comité Interministériel de la Mer, ainsi que le Secrétariat général de la Mer.

55. Il résulte tout d'abord du premier article de ce décret que "Le Comité Interministériel de la Mer est chargé de délibérer sur la politique du Gouvernement dans le domaine de la mer sous ses divers aspects nationaux et internationaux et de fixer les orientations de l'action gouvernementale dans tous les domaines de l'activité maritime". Plusieurs délibérations sont effectuées en sens. En plus du Premier Ministre, y siègent notamment les Ministres de la Défense, de l'Economie et des Affaires étrangères.

56. Ensuite, il résulte de l'article 3 de ce décret que le Secrétariat Général à la mer est placé sous l'autorité du Premier Ministre. Trois missions lui sont principalement attribuées. Tout d'abord, le Secrétariat prépare les délibérations du Comité Interministériel à la Mer. Il veille ensuite à leur exécution. De plus, il participe à une mission de contrôle, d'évaluation et de prospective en matière de politique maritime. Enfin, sous l'autorité du premier ministre, il veille à la coordination de l'action de l'Etat en Mer.

57. Par ailleurs, l'ancien Premier Ministre de la République Française, Manuel Valls, a dévoilé le 16 octobre 2015 la Stratégie Nationale pour la Sécurité du Numérique. Le Premier Objectif de cette stratégie porte sur les intérêts fondamentaux, la défense et la sécurité des Infrastructures Critiques et les Crises Informatiques Majeures. L'objectif est clair : défendre les intérêts fondamentaux de la France dans le cyberespace. Pour ce faire, il sera nécessaire de consolider la sécurité des infrastructures critiques, ainsi que celle des opérateurs essentiels à l'économie.

58. Enfin, le dossier de presse du Comité Interministériel de la Mer en date de 2018 dispose que "La France prend toute la mesure des enjeux liés à la cybersécurité dans le domaine maritime, en termes à la fois de protection des systèmes d'information et de développement économique d'un secteur, et décide ainsi la création d'une Commission cybersécurité et la préfiguration d'un centre national de coordination de la cybersécurité pour le maritime".[12]

59. Ainsi le Comité Interministériel de la Mer et le Secrétariat Général à la Mer ont oeuvré à la création de deux institutions spécialisées : Le Conseil Cyber du Monde

[12] Dossier de Presse. Comité Interministériel de la Mer, 2018.

Maritime, aujourd'hui opérationnel ainsi que le Centre National de la Coordination pour la Cybersécurité pour le maritime, encore en gestation.

Section II - L'élaboration de nouvelles mesures pour la consolidation d'une coordination des acteurs de l'industrie maritime en matière de cybersécurité

60. Suite à l'adoption de la mesure précitée, le Conseil Cyber du Monde Maritime a tenu sa première réunion le 7 novembre 2019 en présence du Secrétaire Général à la Mer, monsieur Denis Robin. Ce conseil a pour objet la mise en place de plusieurs mesures : "la sécurisation du domaine maritime, l'accompagnement des mesures de prévention, de formation et de cyber-résilience, et la création d'un centre national de coordination de la cybersécurité pour le maritime".[13] Il coordonne en outre les acteurs privés et publics, afin d'assurer une meilleure connaissance des attaques menées par les différents adversaires et de rendre l'action collective de l'industrie maritime encore plus forte.

61. Les missions du Conseil ont été précisées de surcroît dans le dossier de presse 2019 du Comité Interministériel de la Mer. Elles sont principalement de deux ordres : l'élaboration de lignes directrices (I), mais surtout la création de nouvelles institutions (II)

I - L'élaboration de nouveaux guides

62. Tout d'abord, est prévue la finalisation de la stratégie de cybersécurité du monde maritime, et par ailleurs, la mise en place d'un guide de bonnes pratiques portuaires avec la direction Générale des Infrastructures des Transports et de la Mer.

[13] Rapport Annuel [en ligne]. Armateurs de France, 2019.

II - La mise en place de nouvelles institutions

63. Ces institutions visent la mise en place de moyens d'actions préventives contre la cybercriminalité, ainsi que de moyens d'actions pour répondre aux attaques lorsqu'elles sont lancées.

A) De nouvelles Institutions pour l'Amélioration de la prévention des cyberattaques

64. Le Comité Interministériel prévoit tout d'abord la création d'un Centre de partage et d'analyse de l'Information. L'objectif est donc ici de renforcer le renseignement en matière de cyberattaque. Cet aspect est absolument fondamental selon monsieur Paul Franquart[14], Autorité Qualifiée en Sécurité des Systèmes d'Information du Grand Port Maritime de Marseille. En effet, si un opérateur est la cible d'un virus, sa responsabilité est d'informer tous les partenaires qui ont un intérêt stratégique. Ils pourront ainsi vérifier, grâce aux caractéristiques communiquées par l'opérateur, si eux-mêmes ont été attaqués. Si aucune communication n'est effectuée, le Grand Port Maritime de Marseille ne pourra jamais savoir s'il a été victime d'agression. Cette ignorance peut être très dangereuse, car si le virus ne peut être détecté, aucune riposte ne pourra le neutraliser[15]. Dans un sondage organisé par IHS en coordination avec le BIMCO, plus 300 personnes du secteur maritime ont été interrogées. Il ressort que 21% des sondés admettent avoir été victimes d'attaques cyber[16]. Toutefois, un auteur estime que ce chiffre est susceptible de ne pas représenter la réalité. En effet, selon cet auteur, il est très vraisemblable que le nombre de victimes soit bien plus élevé car toutes les victimes d'une attaque ne

[14] Autorité Qualifiée en Sécurité des Systèmes d'Information du Grand Port Maritime de Marseille

[15] [audio]. Entretien avec Paul Franquart. 11 mai 2020.

[16] HAND, M. Scale of cyber-security threat against shipping unknown: Bimco. *www.seatrade-maritime.com* [en ligne]. 25 octobre 2016. Disponible à l'adresse : https://www.seatrade-maritime.com/americas/scale-cyber-security-threat-against-shipping-unknown-bimco

souhaiteront pas communiquer à ce sujet en raison du tort qu'elles pourraient causer à la réputation de leur entreprise[17].

65. Il est prévu ensuite la mise en place d'une filière de certification. Selon Bruno Bender[18], l'objectif est d'accréditer d'autres organismes d'une compétence de certification. Aujourd'hui, le seul opérateur de confiance est l'Agence Nationale de la Sécurité des Systèmes d'Information. Cette situation présente deux inconvénients. Tout d'abord, l'exécution de la certification prévue par l'Agence Nationale de la Sécurité des Systèmes d'Information peut selon Bruno Bender être très onéreuse. C'est pourquoi les opérateurs risquent de renoncer à une certification importante pour la consolidation de leur cybersécurité. Si d'autres procédures simplifiées de certification existent, l'ensemble de la chaîne de l'industrie pourra, *in fine,* être protégée. On fermera ainsi l'angle mort résultant de la seule protection des Opérateurs d'Importance Vitale et des Opérateurs de Services Essentiels, notions abordées dans la seconde partie du présent titre.

66. A terme, l'objectif est de créer un Centre National de Coordination pour la Cybersécurité du Maritime.

B) De nouvelles institutions pour l'amélioration de la réponse aux cyberattaques

67. Est tout d'abord préconisée la mise en place d'un centre de réponse d'urgence *(Computer Emergency Response Team)* en cas de cyberattaque ou de compromission

[17] DEVEREESE, G. Considering Cyber Threats in the Maritime Supply Chain. *Maritime Risk International.* 6 juin 2018, n°Juin 2018.

[18] [audio]. Entretien avec Bruno Bender. 31 juillet 2020.

de la cybersécurité sur un navire. Il s'agit ici d'une mise en commun du renseignement et du suivi des cargaisons[19].

68. Sur ce point, monsieur Bruno Bender, coordinateur Cyber auprès du Secrétariat Général à la mer, préconise de surcroît une assistance obligatoire en matière de cybersécurité pour tout navire se situant dans les eaux territoriales françaises.

69. Les seules informations à propos du Conseil Cybersécurité du Monde Maritime ont été données plus haut. Elles seront divulguées et développées lors d'une opération de communication imminente, à ce jour confidentielle, qui va être lancée au salon EURONAVAL 2020[20]

70. L'on a pu voir que le Secrétariat Général à la Mer et le Comité Interministériel œuvrent pour la mise en place d'une coordination des différents acteurs de l'industrie maritime en matière de cybersécurité. Cette coordination comporte notamment la mise en place d'un renseignement efficace pour mieux se prémunir contre les différentes cyberattaques. Elle se concrétise également par une sécurisation des différents acteurs de l'industrie maritime n'entrant pas forcément dans les grandes catégories d'Opérateurs de Services Essentiels et d'Opérateurs d'Importance Vitale qui seront explicitées dans la seconde partie de ce titre. Enfin, l'amélioration de la réaction de l'industrie maritime aux attaques qu'elle subit est également considérée.

71. En plus de cette coordination horizontale, l'établissement d'une sémantique commune pour les acteurs du maritime s'effectue également par la mise à disposition de plusieurs lignes directrices partagées élevées au rang de références. Elles sont

[19] Entretien Précité

[20] [audio]. Entretien avec Bruno Bender. 31 juillet 2020.
; Lettre d'information Cyber Maritime n°3. *https://www.pole-mer-bretagne-atlantique.com/* [en ligne]. Avril 2020. Disponible à l'adresse : https://www.pole-mer-bretagne-atlantique.com/images/C2M2_Lettre_dinformation_CYBER_3_2020.pdf

édictées soit par des organismes étatiques, soit par des instances européennes et internationales.

CHAPITRE 2- L'ÉTABLISSEMENT DE RÉFÉRENTIELS COMMUNS

72. Si la coordination des différents acteurs de l'industrie maritime en matière de cybersécurité s'établit grâce à un dialogue régulier entre eux, un second lien doit être effectué entre ces acteurs et des organismes qui leur sont hiérarchiquement supérieurs, ou qui peuvent être considérés comme des référentiels pertinents s'agissant de l'adoption de mesures techniques. Ce lien permet aux différents acteurs de l'industrie maritime de parler un langage commun en matière de cybersécurité, par- delà les spécificités de chacun. Ces pourquoi les autorités de référence diffusent des guides spécifiques aux objets considérés (Section I), ainsi qu'un ensemble de guides généraux relatifs à n'importe quel système d'information (Section II).

Section I- Les guides spéciaux

73. L'on trouve sur ce point des guides relatifs aux navires et aux installations portuaires. Les recommandations relatives aux navires sont édictées conjointement par la Direction des Affaires Maritimes et la Direction Générale des Infrastructures et des Transports et de la Mer (I). Sur les installations portuaires, la rédaction de lignes directrices nationales est l'un des projets du Comité Interministériel de la Mer. Par ailleurs, L'Agence Européenne de la Sécurité des Réseaux et de l'Information a publié en 2017 un guide des bonnes pratiques de la cybersécurité portuaire (II).

I Les guides relatifs aux navires

74. Le premier guide se concentre sur la protection et l'évaluation du navire (A), tandis que le second approfondit la question de la protection des systèmes industriels du navire (B).

A) Evaluer et protéger le navire

75. L'étude menée "indique les grands axes à suivre pour mettre en place une gestion de la sécurité des systèmes d'information et de communication à bord du navire"[21] [22].

76. Afin d'effectuer des recommandations sur mesure, plusieurs enquêtes sur 68 navires battant pavillon français ont été mises en place.

77. Plusieurs failles ont ainsi été découvertes.

78. Tout d'abord, seuls 32 % des navires sondés faisaient l'objet d'une évaluation des risques de leurs systèmes d'information. 75 % des navires étaient équipés d'un réseau Wifi sans protection. Par ailleurs, dans 69 % des cas, il était possible de relier au réseau du navire un équipement personnel. Cet élément est problématique en raison du fait qu'un équipement personnel peut très vraisemblablement ne pas bénéficier d'une protection identique à celle d'un système d'information.

79. Vis-à-vis de l'hygiène informatique ensuite, deux éléments paraissent problématiques : tout d'abord, la fréquence de changement des mots de passe ne semble pas convenir. En effet, ils ne sont changés régulièrement que dans 18 % des cas. Ensuite, il est estimé qu'ils ne sont pas suffisamment robustes[23] dans 53 % des cas.

80. Enfin, la gestion des droits d'accès à bord du navire parait selon l'étude plus que problématique. En effet, sont classiquement distingués les droits d'utilisateur et les droits d'administrateur. Les droits d'utilisateur permettent en général l'accès à des ressources. Les droits d'administrateur, quant à eux, concernent le fonctionnement du

[21] Evaluer et protéger le navire, Septembre 2016, Direction des Affaires Maritimes, Sébastien Le Vey

[22] LE VEY, S. Evaluer et protéger le navire. Direction Générale des Infrastructures, des Transports et de la Mer/Direction des Affaires Maritimes, Septembre 2016. 3

[23] Le mot de passe est robuste quand il est difficile à deviner et à trouver, notamment avec l'aide d'une attaque par force brute, où des logiciels peuvent essayer plusieurs millions de combinaisons à la seconde, en prenant notamment en compte des éléments trouvés sur des réseaux sociaux

système d'information. Ils permettent notamment la gestion des comptes bénéficiant des droits d'utilisateur, et la maintenance des systèmes. Par conséquent, il est absolument primordial que ces comptes ne soient pas utilisés pour accéder à des logiciels ou des courriels dont la protection est incertaine[24]. Or, selon l'étude de la direction des affaires maritimes, seuls 22 % des systèmes sondés rendent impossible à un compte administrateur la consultation de sites internet ou de courriels[25].

81. La Direction des Affaires Maritimes a donc émis plusieurs recommandations d'ordre général sur l'élévation du niveau de protection. Ces recommandations ont notamment été complétées par le Guide des bonnes pratiques de Sécurité Informatique à bord des navires.

82. Ainsi, sont préconisés sur le plan de la prévention une évaluation du risque, le contrôle régulier du niveau effectif de cybersécurité du navire, ainsi que la surveillance du système.

B) Protéger les systèmes industriels du navire

83. L'objectif est ici celui de la sensibilisation aux risques qu'encourent les systèmes industriels du navire. Le guide préconise ainsi trois étapes clés dans le sens du renforcement de la protection.

84. Le premier niveau consiste en la mise en place d'une stratégie globale de sécurisation. Le but est ici d'apporter un cadre durable pour la sécurisation des systèmes embarqués.

[24] Guide des bonnes pratiques de Sécurité Informatique à bord des navires. Agence Nationale de la Sécurité des Systèmes d'Information, Octobre 2016.

[25] LE VEY, S. Evaluer et protéger le navire. Direction Générale des Infrastructures, des Transports et de la Mer/Direction des Affaires Maritimes, Septembre 2016. 3

85. Le second niveau portera, quant à lui, sur une analyse des risques des différents systèmes.

86. Au premier niveau est préconisé le "durcissement de la chaîne industrielle". Il s'agit de segmenter les réseaux essentiels et de sécuriser en premier lieu l'accès WIFI du navire.

87. S'agissant de la sécurisation de l'accès WIFI au navire, un protocole de chiffrement WPA 2 est préconisé par le guide des bonnes pratiques. Il s'agit de la consolidation du mot de passe et des canaux chiffrés. Pour un attaquant, confronté à un chiffrement WPA 2, il sera difficile d'entrer. Au contraire, si le protocole de chiffrement est faible, le réseau peut être pénétré sans difficulté. Le chiffrement dépend d'un algorithme. Les bons protocoles et le passage par le WPA2 et non par le WEP sont déjà définis par les normes ou le NIST. Ils sont caractéristiques de l'état de l'art et installés par défaut dans le matériel

88. De plus, le paramétrage du système semble un élément tout à fait fondamental.

89. La sécurisation de l'entrée va de pair avec le cloisonnement et une défense en profondeur, c'est-à-dire une multiplication de couches de sécurité, opérée par le VLAN (Virtual Local Area Network) ou Réseau Local Virtuel[26]

90. Si un attaquant parvient à pénétrer dans le système informatique, il sera confronté à un cloisonnement, il n'aura pas accès à tous les réseaux présents sur le navire. A chaque étape d'une attaque, il faut qu'il affronte de nouvelles protections en face de lui. Si l'on a un réseau ouvert avec chiffrement faible, l'adversaire rentre dans le cœur du réseau dès que le chiffrement est décrypté.

[26] Technologie permettant d'obtenir plusieurs réseaux virtuels cloisonnés à partir d'un seul réseau physique

91. Mais si le chiffrement est fort avec un système cloisonné, il va devoir casser le chiffrement, pour entrer dans une zone dont il ne connaît pas la nature, ressortir s'il est arrivé ailleurs qu'à sa cible, faire une nouvelle tentative devant un autre réseau, ce qui lui fait perdre du temps et le rend moins furtif.

92. Le cloisonnement est obtenu grâce aux " virtual local area network", ou réseaux locaux virtuels, qui forment des réseaux dans le réseau. Le grand réseau va être coupé en différents réseaux séparés des autres. Pour passer de l'un à l'autre il faudra des droits. Grâce aux "Public Key Infrastructures", infrastructures à clés publiques, on met en place les règles de segmentation du VLAN. Ainsi, l'on pourra voir un réseau lié à la bureautique, l'autre aux machines, l'autre à la navigation, l'autre au divertissement. Si un marin est dans le divertissement et qu'il n'ait pas de droits d'administrateur puissants, il ne pourra sortir de son activité pour donner des ordres aux machines. Par conséquent, un VLAN pourra être dédié au réseau affecté au divertissement des marins, un autre aux équipements de la navigation. Toutefois, d'autres schémas peuvent également être configurés.

93. Le Guide de sécurité de l'Agence Nationale de la Sécurité des Systèmes d'informations comprend ainsi des recommandations de base, il constitue un socle, dans le but de rendre les attaques plus difficiles. Mais il faut aller plus loin, renforcer encore le socle de sécurité à partir d'une analyse des risques. Le Guide de sécurité ne constitue qu'un minimum vital.

94. Ces guides spéciaux relatifs à la sécurité des systèmes d'Information sont également complétés par une norme plus générale : il s'agit de la norme 27001 de l'Organisation Internationale de Standardisation.

II - Le guide relatif aux infrastructures portuaires

95. L'agence européenne chargée de la sécurité des réseaux et de l'information a publié en 2019 un guide de bonnes pratiques pour la cybersécurité portuaire[27].

96. Si le guide établit les différents opérateurs transitant par l'autorité portuaire, il a également le mérite de recommander de nouvelles technologies permettant la sécurisation des échanges d'information. Y sont notamment mentionnés l'utilisation de la blockchain, ainsi que celle des Infrastructures à clés publiques.

97. La multitude d'acteurs à l'œuvre, l'infinité de transactions se déroulant dans les ports entre navires et autorités portuaires, ainsi qu' entre navires, exigent la plus grande sécurisation des échanges. A cette fin, les guides préconisent la généralisation de technologies récentes, les infrastructures à clés publiques, qui permettent d'échanger des données en toute confidentialité grâce à un tiers de confiance et les blockchains où les échanges se font à l'intérieur d'un groupe délesté d'autorité de garantie, en toute liberté et sécurité.

A) Les infrastructures à clés publiques

98. Comment échanger des messages de manière confidentielle, s'assurer de leur source et de leur intégrité, empêcher leur interception ?

99. L'infrastructure à clés publiques est une réponse dans le domaine des technologies de l'information. Il s'agit d'un ensemble de solutions techniques, basées notamment sur

[27] Port Cybersecurity : Good practices for the maritime sector [en ligne]. Agence Européenne Chargée de la sécurité des réseaux et de l'information, Novembre 2019.

la cryptographie asymétrique, qui impliquent une confiance réciproque avec une autorité de certification.

100. Dans le cadre de la cryptographie asymétrique, chaque utilisateur dispose de deux clés, l'une strictement privée, l'autre totalement publique. La clé publique est issue par hachage de la première, mais ne permet pas de remonter à cette source. Lorsque l'une chiffre un message, seule l'autre peut le déchiffrer.

101. Pour recevoir un message d'une correspondante, appelons-la Iris, un acteur, nommons-le Hermès, lui communique sa clé publique. Grâce à cette clé, Iris chiffrera le message que seul, lui, Hermès, pourra déchiffrer grâce à sa clé privée. Ainsi seront garanties la confidentialité, l'intégrité, l'impossibilité de répudier le message.

102. Pour être assurée de l'identité de son correspondant Hermès, Iris recevra de lui un message en clair, un algorithme de hachage, ainsi que la clé publique. Chacun de son côté, Hermès et Iris obtiendront un même condensat du message en le hachant au moyen du même algorithme. Puis Hermès chiffre par la clé privée le résultat de cette opération : c'est là sa signature. Quand elle l'aura reçue, Iris la déchiffrera avec la clé publique : si le résultat est identique à celui qu'elle avait déjà obtenu, elle aura prouvé l'intégrité et l'authenticité de l'envoi.

103. La communication est donc parfaite entre émetteur et destinataire, à une réserve près, et de taille. Comment s'assurer que la clé publique reçue par la correspondante soit bien celle d'Hermès ? Seul un organisme délivrant un certificat d'authentification pourra assurer que la clé publique correspond bien à l'émetteur. Iris doit donc faire confiance à Hermès, et tous deux doivent se reposer sur l'autorité de certification qui leur accorde sa confiance.

B) La Blockchain

104. Le recours à la nouvelle technologie de la blockchain, initialement à l'œuvre dans les transactions en cryptomonnaie, permet de laisser entrevoir une sécurisation complète des transactions commerciales. Sans entrer dans les détails techniques, on peut définir métaphoriquement la blockchain comme un livre de comptes, également distribués entre tous les utilisateurs, où chaque transaction s'inscrit de manière transparente, indélébile, datée, infalsifiable. Ce système semble écarter la possibilité d'intervention de tiers hostiles. En effet, d'une part, en supprimant le recours à un organe central de confiance, tel qu'une banque, la blockchain enlève à un agent malveillant la possibilité d'investir le centre d'un système pour le désorganiser et en profiter. D'autre part, chacun des utilisateurs est défini par des attributs d'identité liés à une fonction mathématique de hachage qui permet de manière pseudo-aléatoire, grâce à la puissance de calcul de tous les ordinateurs du système, les « mineurs », de laisser une empreinte unique : les identités sont donc infalsifiables.

Section II- Les guides généraux de l'organisation internationale de standardisation

105. La norme étudiée est la norme 27001[28] .

106. Deux familles de normes ISO sont à considérer dans la gestion de la cybersécurité dans l'industrie maritime.

107. La première est la famille de normes 31000. Cette famille de normes se concentre principalement sur la gestion des risques à titre général.

108. La famille des normes 27000 se concentre quant à elle sur la sécurisation des systèmes d'information.

109. La norme 27001 porte sur le management de la sécurité des systèmes d'information. La gestion est organisée selon quatre étapes classiques prévue par la norme 27000, qui offre des éléments de définition pour toutes les normes de cette famille. Les quatre étapes sont les suivantes : Planifier-Faire-Vérifier-Agir (PLAN-DO-CHECK-ACT, en anglais)

110. Cette norme n'est aucunement obligatoire. Toutefois, elle permet d'établir un langage commun des organisations au regard de la sécurité des systèmes d'information.

111. L'objectif de cette norme est d'expliciter les prérequis que doit remplir une organisation pour pouvoir obtenir une certification par l'ISO. Ces prérequis servent à évaluer l'aptitude d'une organisation à être certifiée selon les termes de la norme 27001.

[28] ISO/IEC 27001 MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION. Organisation Internationale de standardisation, Novembre 2013.

I Planifier

1) Contexte de l'organisation

112. Tout d'abord, l'organisation doit relever d'une manière générale "les enjeux externes et internes" (clause 4.1) pertinents et susceptibles d'avoir un poids quant à l'accomplissement d'un système de management et de sécurité de l'information.

113. Ensuite, doivent être déterminées par l'organisation concernée les parties intéressées par le système de management de la sécurité de l'information. Devront également être déterminées les exigences qu'elles devront respecter.

114. Ces deux étapes permettent une première ébauche du domaine d'application du système d'information. Elles seront complétées à la suite de la prise en compte de deux autres éléments : les interfaces par lesquelles passe l'organisation, ainsi que les dépendances existantes entre ses activités et celles menées par d'autres organisations, savoir ses fournisseurs, ses équipementiers, etc., évoqués au point 4.3.

115. Enfin devra être mis en œuvre un Système de management de la sécurité de l'information. Aux termes de la norme, selon le point 0.1, ce système "préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate".

2) Leadership

116. Est visée dans la cinquième clause de la norme la direction de l'organisation.

117. Premièrement, la direction de l'organisation doit affirmer son engagement en faveur des systèmes de management de la sécurité de l'information. Cet engagement se concrétise à travers plusieurs actions. L'on peut notamment citer l'allocation de moyens

et de ressources suffisants, la mise en place d'objectifs et de politiques ou l'intégration des exigences liées aux systèmes de management de la sécurité de l'information au sein des processus métiers (v. Paul Franquart), comme souligné en 5.1.

118. Deuxièmement, la direction d'une organisation devra mettre en place une politique de sécurité de l'information. Celle-ci devra être adaptée aux missions de l'organisation. Elle devra inclure trois éléments : des objectifs de sécurité de l'information, l'engagement d'agir dans le sens d'une amélioration continue de leur sécurité, ainsi que celui de satisfaire aux exigences applicables en matière de sécurité de l'information. Cette politique devra être disponible, communiquée au sein de l'organisation et mise à disposition des parties souhaitant en avoir connaissance. Les objectifs de sécurité obéissent notamment à une cohérence avec la politique de la sécurité de l'information. Ils sont communiqués, mesurés et mis à jour, aux termes du point 5.2.

119. Pour atteindre ces objectifs de sécurité, l'organisation devra déterminer les ressources, la délivrance des résultats, les échéances, les actions exécutées, et les organes responsables de la façon d'atteindre les objectifs de sécurité de l'information, selon le point 6.2.

120. Troisièmement, la direction devra s'assurer d'un élément fondamental : l'attribution puis la communication des responsabilités, des autorités et des rôles concernés par la sécurité de l'information, évoqués à la clause 5.3.

3) Planification de l'évaluation des risques

La clause numéro 6, quant à elle, porte principalement sur l'appréciation des risques.

121. Premièrement, l'organisation doit mettre en place et exécuter un plan d'appréciation des risques. Ce processus établit et tient à jour les critères d'acceptation assumée des risques ainsi que le critère de réalisation de ces derniers. Par ailleurs, il identifie les risques de sécurité de l'information. Sont ici en cause l'identification des risques en lien avec l'intégrité, la confidentialité et la disponibilité des informations relevant du domaine d'application du système de management de la sécurité de l'information. Sont ensuite identifiées les personnes de l'organisation qui auront à faire face à ces risques.

122. Puis les risques de sécurité de l'information sont analysés : les conséquences potentielles en cas d'atteinte à la confidentialité, l'intégrité ou la disponibilité sont appréciées. Par ailleurs, est évaluée la vraisemblance d'apparition des risques. L'organisation procède finalement à une évaluation puis à une hiérarchisation des risques. A l'issue de cette hiérarchisation, sera défini un processus de traitement de risques, prévu au point 6.1.3 où seront déterminées les mesures appropriées pour le traitement des risques de la sécurité de l'information.

4) Support

123. Dans la clause 7, sont prises en compte les ressources, la compétence, la sensibilisation, la communication et les informations documentées.

124. S'agissant des ressources, l'on parle des ressources allouées pour la mise en place, la mise en exécution, la tenue à jour et l'amélioration du système de management de la sécurité de l'information.

125. S'agissant de la compétence, l'on pourrait plus parler de l'aptitude : celle des personnes qui effectuent un travail susceptible de conséquences sur la sécurité du système d'information. Ces compétences seront déterminées par l'organisation, qui

pourra se fonder notamment sur une formation initiale, continue ou une expérience appropriée.

126. Puis, sont considérées les personnes travaillant pour l'organisation. Elles devront faire l'objet d'une sensibilisation à la politique de sécurité précitée. Cette prise de conscience a pour objet de se rendre compte que chaque personne travaillant pour l'organisation contribue à l'efficacité du système de management de la sécurité de l'information.

127. Par ailleurs, est traitée la détermination des besoins de communication pertinents pour le système de management de la sécurité de l'information. Il faudra déterminer quand communiquer, comment le faire, avec qui et surtout à quel sujet.

128. S'agissant enfin des informations documentées, Le système de management de la sécurité de l'information inclut les informations documentées exigées par la Norme 27001, mais aussi les informations documentées que l'organisation juge nécessaires à l'efficacité du système de management de la sécurité de l'information. (Le dépassement des normes ISO peut être nécessaire). En outre, dans un objectif de clarté, les informations sont vérifiées et approuvées selon leur caractère approprié et leur pertinence. Les documents devront également être protégés. En dernier lieu, selon le point 7.5.3., pour contrôler les informations documentées, l'organisation devra, lorsqu'elle est compétente, traiter la préservation, la lisibilité, la durée de conservation et de la suppression de ces informations.

II Faire

129. Trois éléments sont pris en compte dans la 8ème clause : la mise en place de processus de contrôle opérationnels, ainsi que l'appréciation puis le traitement des risques de sécurité de l'information.

130. Tout d'abord, les processus mis en place répondent principalement à un objectif, la réalisation des actions déterminées dans la clause 6.1, ce dans le but d'atteindre les objectifs de sécurité, mis en place conformément à la clause 6.2.

131. Ensuite, l'organisation doit contrôler les modifications du système de sécurité de l'information. Seront ensuite analysées les conséquences des modifications qui n'avaient pas été prévues. L'organisation devra alors œuvrer pour une limitation de leur éventuel effet négatif.

132. Par ailleurs, l'organisation doit réaliser des appréciations des risques de sécurité à intervalles réguliers, ou alors lorsque des changements significatifs sont prévus ou ont lieu, en tenant compte des critères établis en 6.1.2 a).

133. Enfin, il incombe à l'organisation d'exécuter un plan de traitement des risques de sécurité de l'information.

III Vérifier

134. En premier lieu, il incombe à l'organisation d'évaluer non seulement les performances de sécurité de l'information, mais aussi de mesurer l'efficacité de la gestion de cette dernière. Pour ce faire devront être déterminés les points à surveiller ainsi que les méthodes de surveillance. Devront également être prévus les intervalles de ces contrôles, ainsi que les personnes qui les effectueront. Elles pourront ensuite analyser et évaluer les résultats.

135. En second lieu, l'organisation doit se faire auditer à des intervalles planifiés. L'objectif est de déterminer si le système de management de la sécurité de l'information est conforme aux exigences propres de l'organisation, ainsi qu'à celles de la norme 27001. Le périmètre des audits doit être tracé par l'organisation. En outre, doivent être sélectionnés des auditeurs dont l'objectivité et l'impartialité sont garanties.

136. En dernier lieu, à des intervalles planifiés, la direction doit mettre en place une revue du système de management de la sécurité de l'information.

137. Cette revue de la direction prend en compte plusieurs éléments. Est notamment évalué l'état d'avancement des actions décidées à l'issue des revues de direction précédentes. Par ailleurs, sont analysés les retours sur les performances de sécurité de l'information, concernant notamment les non-conformités du système, les résultats des audits et des actions correctives, ainsi que la réalisation des objectifs en matière de sécurité de l'information.

IV Agir

138. La dixième clause de la norme a finalement trait à l'amélioration des systèmes, suite à la mise en place des trois actions précédentes.

139. Lorsqu'une non-conformité apparaît, l'organisation doit la maîtriser et la corriger. Sera ensuite évaluée la nécessité de mener une action pour éliminer les causes de la non-conformité. Celle-ci fait donc l'objet d'une procédure bien définie.

140. Par conséquent, l'organisation examine la non-conformité, en détermine les causes, puis vérifie si des non-conformités similaires impactent déjà le système d'information de l'organisation.

141. Il faut ensuite réviser les actions correctives et leur efficacité. Puis, si cela est nécessaire, sera modifié le système de management de la sécurité de l'information.

142. Enfin, les documents issus des procédures susmentionnées devront être conservés. Ainsi, une preuve de la nature des éventuelles non-conformités, comme les résultats de toute action corrective, pourra être consultée.

143. Ainsi, la norme ISO 27001 pose les lignes de conduite adéquates pour la mise en place d'un Système de Management pour la sécurité de l'information. Le processus PLAN-DO-CHECK-ACT porte sur une mise en place de la sécurisation de l'information au sein d'une seule et même organisation. Toutefois, selon Fabien Caparros, il n'est pas suffisant face au risque cyber actuel. La raison de cette insuffisance tient notamment au fait que le risque cyber est seulement considéré dans une dimension technique. Cette approche contribue à une tentative de résolution de ce risque par la création de "citadelles". Cela signifie que lorsqu'une organisation essaie de résoudre ce qui est à ses yeux un problème technique, l'objectif sera d'identifier et de réparer plusieurs vulnérabilités. Cela était jadis suffisant. En effet, lors de l'édiction de la norme, en 2013, les attaquants prenaient pour cible les entreprises grâce à des vulnérabilités techniques connues. Tel n'est plus le cas aujourd'hui. En effet, les attaquants se concentrent davantage sur les vulnérabilités les plus récentes qui n'ont pas fait l'objet de correctifs de la part de l'administrateur du système[29].

144. Ainsi, l'appréhension de la problématique cyber sous un prisme exclusivement technique déconnecte la protection de la réalité des menaces. La défense élaborée manque d'agilité[30].

145. Par ailleurs, les approches basées sur les normes ISO, lorsqu'elles sont pauvrement exécutées, ne prennent pas en compte l'écosystème dans lequel s'insère le système d'information de l'organisation considérée.

[29] Il peut ici s'agir soit d'une faille 0-day, soit du manquement de l'administrateur à exécuter le correctif. Dans le cadre de la faille 0-Day, la vulnérabilité considérée est soit inconnue, soit irrésolue. S'il s'agit d'un manquement de l'administrateur à exécuter le correctif, la faille est connue, un remède existe, mais l'on n'a pas exécuté ce dernier en raisons de biais psychologiques et processuels, qui sont abordés dans la deuxième partie de ce mémoire.

[30] Capacité à évoluer afin de s'adapter aux nouveaux contextes dans lesquels se trouve le système d'information considéré.

146. Par conséquent, la norme pourra établir un référentiel de base qu'il ne faudra pas délaisser. Toutefois, une cybersécurité efficace supposera la mise en place d'éléments supplémentaires pour appréhender au mieux le risque cyber couru par une organisation.

147. En guise de conclusion, l'on a pu voir que la nécessaire coordination des acteurs de l'industrie maritime est à peine en cours d'élaboration grâce aux travaux du Secrétariat Général à la Mer et du Comité Interministériel de la Mer. Par ailleurs, plusieurs organismes tel que la Direction des Affaires Maritimes, l'Agence Européenne chargée de la Sécurité des réseaux et de l'Information, et la famille de normes de l'Organisation Internationale de Standardisation permettent l'établissement d'une sémantique commune pour une protection effective contre la cybercriminalité. Il n'en demeure pas moins que, théoriquement à tout le moins, l'établissement d'une cybersécurité pour chacun des acteurs de l'industrie maritime s'effectue individuellement, au sein de chacune des entités concernées. Ainsi, chacun des différents acteurs sera apte à mettre en place une sécurisation des systèmes d'information au regard de sa propre architecture. Afin de mener à bien cet objectif, un droit commun pour chacun des acteurs devra donc être mis en place afin d'assurer la gestion organique et atomisée de la cybersécurité dans l'industrie maritime.

TITRE II LA SUFFISANCE DU SOCLE EN VIGUEUR POUR LA GESTION ORGANIQUE ET ATOMISÉE DE LA CYBERSÉCURITÉ DANS L'INDUSTRIE MARITIME

148. Comme nous l'avons vu dans l'introduction de ce mémoire, la cybersécurité dans l'industrie maritime reste un domaine en construction. Cet aspect inachevé se révèle également dans l'établissement de bases légales encadrant la cybersécurité maritime. L'Agence Européenne Chargée de la Sécurité des Réseaux et des Systèmes d'Information le faisait remarquer en 2011 dans son rapport initial lié à la cybersécurité maritime [31]. Il était en effet considéré que le droit positif de l'époque[32] ne prenait en compte que les aspects physiques de la sûreté maritime. Les cyberattaques n'étaient donc pas considérées, selon le rapport, comme des menaces issues d'agissements illégaux. Les cadres légaux n'étant pas suffisamment définis, les différents modèles de cybersécurité étaient librement choisis par chacune des entités de l'industrie maritime, la mise en place d'une cybersécurité dépendait entièrement des acteurs opérationnels désignés par chaque organisation. Les connaissances des personnes devant faire face à d'éventuelles attaques étaient donc limitées, peut-être même les différentes mesures envisageables n'étaient-elles pas connues.

[31] Analysis of Cyber Security Aspects In the Maritime Sector. Agence Européenne Chargée de la Sécurité des Réseaux et de l'Information, 19 Décembre 2011.

[32] Il est notamment fait référence au règlement n°725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, au Code International pour la Sûreté du Navire et autres Installations Portuaires

TITRE II LA SUFFISANCE DU SOCLE EN VIGUEUR POUR LA GESTION ORGANIQUE ET ATOMISÉE DE LA CYBERSÉCURITÉ DANS L'INDUSTRIE MARITIME

149. Cette absence de droit commun relatif à la cybersécurité maritime est aujourd'hui, comme nous allons le voir, bien moins criante aussi bien dans l'Union Européenne qu'en France.

CHAPITRE I- UN DROIT EN COURS D'ÉLABORATION : L'APPORT DE L'ORGANISATION MARITIME INTERNATIONALE

150. Si un droit commun est aujourd'hui en vigueur (Chapitre 2), un droit en cours d'élaboration dont les modalités d'exécution restent floues est également disponible (Chapitre I).

151. Si cette partie n'est pas incluse dans le second chapitre qui traite du droit positif applicable en France et dans l'Union Européenne, cela tient au fait que les modalités de transposition des normes de l'Organisation Maritime Internationale par les Etats membres restent inconnues. En effet, les recommandations finales ne seront dévoilées que le 1er janvier 2021.

152. Il faut donc tout d'abord analyser les mesures énoncées par l'Organisation Maritime Internationale (Section I). Puis, au sein de ces mesures, les références à d'autres normes édictées par l'Organisation maritime internationale, qui ont déjà permis une relative prise en compte de la cybersécurité par les armateurs (Section II).

Section I - La prise en compte de la Cybersécurité par l'Organisation Maritime Internationale

153. Le 5 juillet 2017, l'Organisation Maritime Internationale publie des lignes directrices sur la gestion du risque cyber maritime[33]. Dans ces lignes directrices, sont reprises notamment les cinq étapes préconisées par le NIST Security Framework pour gérer efficacement le risque cyber.

[33] Organisation Maritime Internationale, *n°MSC-FAL.1-Circ. 3 Guidelines on Maritime Cyber Risk Management* en ligne. 5 juillet 2017.

154. Les 5 étapes sont : l'Identification, la Protection, la Détection, la Réponse et le Rétablissement.

155. L'Identification consiste en la qualification des rôles et responsabilités du personnel pour la gestion du risque cyber ainsi qu'en l'identification des systèmes, biens, données et capacités qui, lorsqu'ils sont perturbés, posent un risque aux opérations du navire.

156. La protection, quant à elle, consiste en la mise en place de processus et de mesures relatives au contrôle du risque, et l'établissement de plans d'urgence, afin de défendre un système contre un incident cyber, en vue de garantir la continuité des opérations liées au transport maritime.

157. Outre certaines recommandations, est effectué un renvoi à plusieurs normes. Si cette liste n'est pas limitative, le NIST Framework Américain, la norme ISO 27001 et les lignes directrices pour la cybersécurité à bord du navire[34] sont clairement mentionnés.

158. Puis, par la résolution MSC.428 en date du 16 juin 2017, l'Organisation maritime Internationale consacre une certaine prise en compte effective de la gestion du risque cyber au sein des compagnies maritimes.

159. En effet, l'Organisation Maritime Internationale affirme d'abord qu'un système de gestion de sécurité[35] approuvé devra prendre en considération la gestion du risque cyber

[34] The Guidelines on Cyber Security Onboard Ships [en ligne]. BIMCO, CLIA, ICS, INTERTANKO, INTERCARGO, IUMI, INTERMANAGER, OCIMF, World Shipping Council, 2018.

[35] Safety Management System

en conformité avec les objectifs et prérequis fonctionnels du Code International de Gestion de Sécurité.

160. Puis l'Organisation Maritime Internationale encourage les administrations à garantir que les risques cybernétiques soient pris en considération dans leur système de gestion de sécurité, au plus tard lors de la première vérification du Document de Conformité qui doit avoir lieu après le 1er janvier 2021.

161. Cette résolution paraît hybride. En effet, si elle ne fait qu'encourager les administrations à garantir que le risque soit pris en considération, elle affirme que pour être approuvé, le système de gestion de sécurité devra prendre en compte la gestion du risque cybernétique.

Section II- Les normes d'exécution de l'Organisation maritime Internationale

162. Suite à cette résolution, il convient d'analyser en quoi le risque cybernétique peut être inclus dans le cadre des dispositions du Code International de Gestion de la Sécurité (I). Par ailleurs, les différentes dispositions du Guide sur la cybersécurité à bord des navires devront être analysées car les recommandations données englobent largement les activités de l'armateur liées à la cybersécurité (II)

I La prise en compte du risque cyber par le Code International de Gestion de la Sécurité.

163. Le 4 novembre 1993, l'Assemblée Générale de l'Organisation Maritime adopte le Code International de Gestion pour la sécurité des navires et pour la prévention de la pollution. Puis, le Code est incorporé en 1994 à la Convention pour la Sauvegarde de la Vie Humaine en Mer. Cette inclusion lui confère un caractère obligatoire pour tout navire de plus de 500 tonneaux de jauge brute, ainsi que pour tout navire à passagers.

L'un des apports principaux de ce Code est de rendre obligatoire pour l'armateur un système de gestion de la sécurité.

164. Aux termes de l'article 1.1.4 du Code, il s'agit d'un système structuré et documenté permettant au personnel de la compagnie d'appliquer efficacement la politique de la compagnie en matière de sécurité et de protection de l'environnement.

165. Aux termes de l'article 1.2.3 du Code ISM, le système de gestion de sécurité a pour objectif de garantir deux éléments.

166. Tout d'abord, il garantit le respect des règles et règlements obligatoires. Puis il garantit la prise en considération des recueils de règles, codes, directives et normes applicables qui font l'objet d'une recommandation par l'Organisation Maritime Internationale, les Administrations, les sociétés de classifications et les organismes du secteur maritime.

167. Cet objectif doit de surcroît être mis en pratique. En effet, aux termes de l'article 1.4 du Code, il incombe à la compagnie maritime de mettre en place un système de gestion de la sécurité qui comporte notamment une politique en matière de sécurité, des procédures d'audit interne et de maîtrise de la gestion. Sont également prévues des instructions et des procédures concernant la sécurité des opérations à bord. La liste donnée par le Code n'est nullement limitative.

Selon Saleha Ouhadj, ces procédures doivent être simples.[36] En effet, elles visent, semble-t-il, à être appliquées à la lettre pour une sécurisation optimale.

[36] OUHADJ, S. *La Mise en Application de l'ISM Code par les Compagnies* [en ligne]. Mémoire pour l'Obtention du D.E.S.S en Droit Maritime et des Transports : Aix-en-Provence : Aix-Marseille/Centre de Droit Maritime et des Transports. 1999

168. Pour faciliter leur exécution, elles devront notamment être courtes et en nombre réduit. Il faudra enfin que des administrateurs des affaires maritimes ou des sociétés de classification analysent à bord les pratiques déjà en place sur le navire. Si les prescriptions du code ISM sont respectées, deux documents seront alors délivrés à la compagnie maritime par l'état du pavillon, tout d'abord le document de conformité, ensuite un certificat de gestion de la sécurité attestant que le personnel d'encadrement à bord de chaque navire de la compagnie l'exploite conformément au système de gestion de sécurité. En France, la demande initiale de certification devra être adressée à la Direction des affaires Maritimes.

169. Comme nous l'avons vu précédemment, l'Organisation Maritime Internationale subdivise dans son guide en date du 5 juillet 2017[37] la gestion maritime des risques cybernétiques en 5 étapes. Celle de l'Identification consiste en la qualification des rôles et responsabilités du personnel pour la gestion du risque cyber et en l'identification des systèmes, biens, données et capacités qui présentent un risque pour les opérations du navire lorsqu'ils sont perturbés.

170. Celle de la protection quant à elle suppose une mise en place de processus et de mesures relatives au contrôle du risque, et l’établissement de plans d’urgence afin de défendre un système contre un incident cyber, dans le but de garantir la continuité des opérations

[37] Organisation Maritime Internationale, *n°MSC-FAL.1-Circ. 3 Guidelines on Maritime Cyber Risk Management* en ligne. 5 juillet 2017.

II Les mesures d'exécution concrètes de prises en compte du risque cyber

A) L'identification

1) Détermination des rôles et des responsabilités

171. L'article 3.2 du Code ISM dispose que " La compagnie devrait définir et établir par écrit les responsabilités, les pouvoirs et les relations réciproques de l'ensemble du personnel chargé de la gestion, de l'exécution et de la vérification des activités liées à la sécurité et à la prévention de la pollution ou ayant une incidence sur celles-ci.".

172. En termes de risques cyber, la prise en compte de cette obligation comprend la prise en compte de la différence entre les Technologies de l'Information et la Technologie opérationnelle. Les Technologies de l'Information gèrent les données virtuelles, tandis que les technologies opérationnelles contrôlent les aspects physiques de la cybersécurité. En d'autres termes, les technologies opérationnelles concernent les logiciels et matériaux informatiques, les procédés et appareils physiques. Les technologies de l'information se concentrent uniquement sur le traitement de l'information.

173. Les deux domaines étaient traditionnellement séparés. Toutefois, de plus en plus d'équipements sont connectés à Internet. Ainsi, les technologies de l'Information et les Technologies opérationnelles sont de plus en plus imbriquées. Une politique améliorée de protection de la sécurité devra tout d'abord démontrer que la gestion des risques cyber s'inscrit dans l'approche globale de la gestion de la sécurité. Ensuite, devront être pris en compte aussi bien les aspects du risque cybernétique liés à la sécurité que ceux liés à la sûreté. Les enjeux de la sécurité seront hiérarchiquement plus importants.

174. Par ailleurs, l'article 3.3 du Code ISM dispose que "La compagnie doit veiller à ce que des ressources adéquates et un soutien approprié à terre soient fournis pour que la ou les personnes désignées puissent s'acquitter de leurs tâches".

175. Il a été mentionné plus haut la dichotomie entre les Technologies de l'Information et les Technologies opérationnelles.

176. Cette dichotomie ne doit pas se transformer en obstacle contre la mise en place de la cybersécurité. En effet, les départements spécialisés dans la technologie de l'information bien souvent ne s'occupent pas de l'achat de technologies opérationnelles. Ces départements doivent se concentrer sur les potentielles vulnérabilités des systèmes informatiques et connaître les procédures adéquates pour endiguer ces vulnérabilités dans l'objectif d'une protection des données. Dès lors, l'achat de technologies opérationnelles sera effectué par le chef mécanicien. Les connaissances de ce dernier risquent de ne pas être axées sur la gestion du risque cyber ou sur la sécurisation des logiciels. Elles se concentreront davantage sur l'impact des objets à bord sur le fonctionnement du navire. Par conséquent, avant l'achat des différentes technologies opérationnelles, le guide recommande instamment qu'un dialogue ait lieu entre les responsables de technologies de l'information et ceux des technologies informationnelles, afin qu'il soit garanti que la cybersécurité des technologies opérationnelles soit prise en compte durant leur achat. Dès lors, devront être mises en place des autorités tierces encourageant la coopération entre ces deux départements.

177. Enfin, l'article 6.5 du Code ISM dispose que " La compagnie devrait établir et maintenir des procédures permettant d'identifier la formation éventuellement nécessaire pour la mise en œuvre du système de gestion de la sécurité et veiller à ce qu'une telle formation soit dispensée à l'ensemble du personnel concerné. "

178. Sur ce point, le guide insiste sur le fait que l'entraînement du personnel est une mesure clé formant la base de la gestion du risque cyber. En effet, l'entraînement garantit une prise de conscience des équipages quant aux conséquences qu'implique chacune de leurs actions. Les procédures relatives à l'établissement de besoins d'entraînement devraient donc être mises à profit pour des cours de cyber-sensibilisation destinés à l'ensemble du personnel de la compagnie maritime.

2) Identification des systèmes et données critiques

179. L'article 10.3 du Code International de Gestion de la Sécurité dispose que " La compagnie devrait établir dans le cadre du système de gestion de la sécurité des procédures permettant d'identifier le matériel et les systèmes techniques dont la panne soudaine pourrait entraîner des situations dangereuses. Le système de gestion de la sécurité devrait prévoir des mesures spécifiques pour renforcer la fiabilité de ce matériel et de ces systèmes. Ces mesures devraient inclure la mise à l 'essai à intervalles réguliers des dispositifs et du matériel de secours, ainsi que des systèmes techniques qui ne sont pas utilisés en permanence ".

180. Dans une transposition de cette disposition au risque cyber, cette étape implique tous les équipements -aussi bien ceux liés à la technologie Informationnelle que ceux liés à la technologie opérationnelle- qui peuvent causer des situations dangereuses si leur fonctionnement est perturbé. En plus de cette exigence, il faut également prendre en compte que la perte de disponibilité ou d'intégrité des données utilisées par des systèmes critiques peut impacter la sécurité du navire. Dès lors, la liste des équipements et des systèmes techniques devra également comporter les données utilisées par ces derniers. Enfin, les sources devront également être mentionnées.

181. A l'issue d'une identification exhaustive des risques et de leur traitement par les différents organes de la compagnie, la protection des systèmes du navire pourra ensuite être considérée.

B) Protéger

182. L'étape de la protection prévue par l'Organisation Maritime Internationale dans ses lignes directrices consiste en la mise en place de processus et de mesures relatives au contrôle du risque, et l'établissement de plans d'urgence afin de défendre un système contre un incident cyber, en vue de garantir la continuité des opérations liées au transport maritime.

1) Mise en place du contrôle du risque

183. L'article 1.2.2 indice 2 du Code International de Gestion de la Sécurité dispose que les objectifs de la compagnie en matière de gestion de la sécurité doivent notamment établir des mesures de sécurité contre tous les risques identifiés.

184. Cette partie a trait à la défense en profondeur, ainsi qu'à la défense en largeur du système d'information.

185. La défense en profondeur du système d'information est une défense globale et dynamique. Elle coordonne plusieurs lignes de défense qui couvrent toute la profondeur du système, c'est à dire dans l'organisation et la mise en œuvre du système d'information, comme dans les technologies utilisées. [38]

186. Cette défense s'accompagne d'une défense en largeur, qui se concrétise par un ensemble d'activités ayant pour objectif d'identifier, de gérer et de réduire les failles

[38] La défense en profondeur appliquée aux systèmes d'information. Direction centrale de la sécurité des Systèmes d'Information, 19 juillet 2004.

exploitables dans les systèmes des technologies de l'information, ainsi que dans ceux des technologies opérationnelles. Par conséquent le guide, préconise notamment des mesures de base à effectuer avant même l'évaluation du risque. Ainsi seront inventoriés les logiciels et les équipements. Puis il est recommandé que les équipements soient maintenus à condition que les configurations de sécurité maintenues pour eux soient en conformité avec l'état de l'art.

187. Enfin, des mesures quant à la restriction de l'accès aux équipements critiques du navire devront également être prises en compte.

2) Mise en place de plans d'urgence

188. L'article 7 du Code International de Gestion de la sécurité dispose que "la compagnie devrait définir les procédures à suivre pour l'établissement de plans et de consignes, y compris de listes de contrôle, s'il y a lieu, pour les principales opérations à bord concernant la sécurité du navire et la prévention de la pollution. Les diverses tâches en jeu devraient être définies et assignées à un personnel qualifié".

189. Si la gestion du risque cyber ne devrait pas impacter a priori les plans déjà mis en place pour la sécurité à bord du navire, des instructions à mettre en œuvre en cas d'attaque d'un système critique devront être mises en place.

190. En ce sens, l'article 8.1 du Code International de Gestion de la Sécurité dispose que "la compagnie devrait établir les procédures pour identifier et décrire les situations d'urgence susceptibles de survenir à bord ainsi que les mesures à prendre pour y faire face".

191. Certains plans d'urgences sont souvent mis en place dans le cadre du système de gestion de sécurité, notamment pour le cas d'incendie. Le guide préconise ici une formation relative à des incidents liés au cyber. Cette formation serait intégrée avec

l'ensemble des autres formations mises en place dans le cadre du système de gestion de sécurité. Les incidents susceptibles de constituer l'objet de la formation du personnel de la compagnie maritime pourront notamment être la perte de disponibilité des équipements électroniques liés à la navigation. Un autre incident pouvant faire l'objet d'une formation est notamment celui du "rançongiciel", c'est à dire un logiciel malveillant d'extorsion, prenant en otage des données indispensables, jusqu'au versement d'une somme d'argent.

CHAPITRE 2- LE DROIT POSITIF APPLICABLE À LA CYBERSÉCURITÉ DANS L'INDUSTRIE MARITIME

193. Depuis le début des années 2010, les problématiques de cybersécurité ont été investies par les institutions étatiques et européennes. A ce titre, l'Union Européenne a adopté la directive 2016/1148 du Parlement européen et du Conseil 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.

194. Avant cette directive, la France a adopté la 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.

Section I - Le Droit de l'Union Européenne

195. Outre l'inscription des risques cyber dans le giron de la sécurité maritime, ce risque est également pertinent dans le cadre de la sûreté maritime. A ce titre, l'article B8.3 du Code international pour la sûreté des navires et des installations portuaires dispose que l'évaluation de süreté du navire doit également porter sur systèmes de radio et télécommunications, y compris les systèmes et réseaux informatiques. Cette disposition a été reprise dans le règlement n° 725/2004 du Parlement Européen et du Conseil en date du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires. Le champ d'application de ce règlement a été repris dans la directive 2016/1148 du Parlement européen et du Conseil 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.

I Objectifs et définitions

196. Le premier alinéa de l'article 1 établit clairement l'objectif de la directive NIS : « assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur ».

197. Le second alinéa prévoit la mise en place de cinq types de mesures. Certaines ont trait à l'élaboration d'une stratégie nationale en matière de cybersécurité. D'autres ont pour objectif une coordination des actions des différents états membres de l'Union Européenne

A) Les prescriptions pour l'adoption de stratégies nationales et de coordinations interétatiques

Stratégies nationales

198. Tout d'abord, est fixée par la directive un cadre pour les Etats membres pour l'adoption d'une stratégie nationale en matière de cybersécurité.

199. Les Etats devront ensuite se doter d'autorités nationales en matière de sécurité des réseaux et des systèmes d'informations.

200. Finalement, la directive consacre l'obligation pour les Etats de créer des centres de réponse aux incidents de sécurité informatiques, ou les CSIRT (en anglais : Computer Security Incident Response Team).

Coordination interétatique

201. Les états membres devront désigner des autorités nationales compétentes et des points de contact uniques pour les tâches liées à la sécurité des réseaux et des systèmes d'information.

202. Enfin, les CSIRT des différents états membres devront coopérer entre eux.

B) La régulation de deux acteurs extra-étatiques : Les Opérateurs de service essentiels et les Fournisseurs de services numérique*s*

203. L'article 1 alinéa 2 indice d) affirme que la Directive a pour objectif d'établir "des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels et pour les fournisseurs de service numérique".

II Mise en œuvre des objectifs de la directive.

A) Mise en place des CSIRT

204. L'article 9 de la directive NIS impose aux Etats membres la désignation d'un ou plusieurs CSIRT. Aux termes du 1er point de l'annexe 1 de la directive, ces derniers devront bénéficier de sites sécurisés. Ils devront en outre assurer une continuité des opérations, avec des effectifs appropriés pour assurer une disponibilité permanente. Les demandes seront gérées avec un système de gestion et de routage afin de faciliter leurs transferts. De plus, les CSIRT bénéficieront d'une infrastructure à la continuité garantie par les Etats membres, qui, au terme de l'article 9 alinéa 2 de la directive, veilleront à ce que les CSIRT soient pourvus de ressources suffisantes, nécessaires pour être opérationnels au niveau des tâches qui leur seront confiées. Finalement, les Etats

membres doivent informer la Commission des CSIRT qu'ils ont mis en place, ainsi que des missions confiées.

1) Obligations des CSIRT

205. Il faut ici se référer à l'article 9 de la directive, qui effectue un renvoi au 2ème alinéa de l'annexe I. Aux termes de ce dernier, les CSIRT ont a minima cinq tâches. Ils effectuent premièrement "un suivi des incidents au niveau national". Dans le cadre de cette directive, est un incident « tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information ». Ils activent deuxièmement le mécanisme d'alerte précoce, diffusent des messages d'alerte, puis effectuent des annonces et des diffusions d'informations sur les risques et incidents auprès des parties intéressées. Troisièmement, ils interviennent en cas d'incident. Ils effectuent quatrièmement une analyse dynamique des risques et incidents. Finalement ils participent au réseau des CSIRT.

206. Par ailleurs, les CSIRT coopèrent avec le secteur privé. Pour ce faire, ils promeuvent des procédures de gestion des risques et incidents, ainsi qu'une classification de ces derniers.

2) Coopération des CSIRT

207. L'article 12 de la directive prévoit la mise en place d'un réseau des CSIRT, dont les lignes directrices sont fournies par les différents Etats membres.

208. Les représentants des CSIRT des Etats Membres et le CERT-UE forment le réseau des CSIRT

209. Les missions principales confiées au réseau des CSIRT ont trait à l'échange d'informations. Il est question tout d'abord d'informations sur « les services, les opérations et les capacités de coopération des CSIRT ».

210. Par ailleurs, sont visées les informations relatives à un incident transfrontalier, en cours, ou identifié, sous réserve que les informations ne sont pas sensibles ou confidentielles.

211. En outre, le réseau étudie les recommandations effectuées par l'ENISA, l'Agence européenne chargée de la sécurité des réseaux et de l'information.

212. Enfin, il se charge de publications de lignes directrices en vue de faire converger les pratiques concernant l'application des dispositions de l'article 12.

B) Les fournisseurs de service numériques

213. La définition des fournisseurs n'est pas précisée par la directive. En effet, il est seulement affirmé dans l'article 11 qu'il s'agit d' « une personne morale fournissant un service numérique ».

1)Compétence des Etats membres

214. Aux termes du premier alinéa de l'article 18 de la directive, un FSN relève de la compétence d'un Etat membre où il a son siège social. En effet, dès lors que le siège social se trouve dans un Etat membre, l'établissement principal du FSN est alors déterminé.

215. Par ailleurs, il ressort de l'article 18 alinéa 2 qu'un Etat membre peut être compétent au regard d'un FSN si celui-ci y fournit un des trois services suivants : au terme de l'annexe III de la directive, si une place de marché en ligne, un moteur de recherche en ligne ou un service informatique en nuage est fourni, la compétence de l'Etat membre peut être établie.

216. Le FSN devra alors nommer un représentant dans un Etat membre, qui sera alors compétent.

2) Encadrement des FSN par les Etats membres

217. L'encadrement des Etats porte sur trois éléments. Tout d'abord, l'encadrement porte sur l'identification des risques menaçant la sécurité des réseaux et des systèmes d'information utilisés pour offrir les services prévus par l'annexe III susmentionnée. Est ainsi garantie la sécurité des réseaux et des systèmes d'information. Par conséquent, les mesures prennent en considération la gestion des incidents et la continuité des services, la sécurité des systèmes et installations, le respect des normes internationales, le suivi, l'audit et le contrôle.

218. Ensuite, l'encadrement porte sur l'adoption par les FSN de mesures permettant d'éviter les incidents, d'en réduire les impacts, afin de garantir la continuité des services. Finalement, les Etats membres doivent contrôler que les FSN notifient aux autorités compétentes ou au CSIRT les incidents portant un impact significatif sur la fourniture d'un service. De surcroît, les notifications doivent indiquer les éléments permettant au CSIRT d'évaluer l'ampleur de l'impact considéré.

219. L'objectif est que ces mesures consolident un niveau de sécurité des réseaux et des systèmes d'informations. Pour ce faire, sont pris en considération cinq éléments : le nombre d'utilisateurs touchés par l'incident, la durée de ce dernier, sa portée géographique, la gravité de la perturbation sur le fonctionnement du service et l'ampleur de l'impact sur les fonctions économiques et sociétales. [39].

220. Sur le plan de l'exécution de ces encadrements, il résulte de l'article 17 de la directive que les autorités compétentes peuvent imposer aux FSN la communication des informations nécessaires pour l'évaluation de la sécurité de leurs réseaux et systèmes d'information. Font partie de ces informations les documents internes en lien avec leur politique de sécurité.

221. Aux termes de l'article 16 de la directive, « les États membres veillent à ce que les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union, les services visés à l'annexe III, et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer ».

[39] Article 16, alinéa 4.

3) La hiérarchisation entre l'encadrement des fournisseurs de service numérique et celui des Opérateurs de Services Essentiels

222. Il faut ici se référer au considérant 49 de la directive NIS. Ce dernier affirme en premier lieu un principe de proportionnalité entre le niveau de sécurité fourni par le FSN et le risque menaçant la sécurité des services proposés, ce en raison du caractère important des services proposés pour les activités des autres entreprises au sein de l'Union.

223. Puis est effectuée en second lieu une distinction entre le degré de risque encouru en pratique par les opérateurs de services essentiels et celui encouru par les fournisseurs de service numériques. Ces derniers encourent un degré de risque moins élevé que les opérateurs de service essentiels. En effet, les OSE constituent, selon ce considérant, un élément crucial pour le maintien de fonctions sociétales et économiques critiques.

224. Par conséquent, les exigences en matière de sécurité imposées aux fournisseurs de services numériques devraient être moins strictes.

225. En découle donc une certaine liberté pour les fournisseurs de services pour prendre les mesures qu'ils estiment pertinentes dans la gestion des risques mettant en péril la sécurité de leurs réseaux et de leurs systèmes d'information.

226. Dès lors, les FSN devront mettre en place des mesures nécessaires et proportionnées pour gérer les risques capables de compromettre la sécurité des réseaux et des systèmes d'information.

227. Est préconisée toutefois une approche plus harmonisée des FSN au niveau de l'Union. En effet, leurs activités sont par nature transfrontalières. Cette approche est définie et mise en œuvre au travers des moyens d'actes d'exécution.

228. Il faut donc retenir que les OSE ont un fonctionnement encore plus encadré que celui des FSN. Cet élément est fondamental, car il vise directement, comme nous allons le voir, les acteurs de l'industrie maritime.

C) Les Opérateurs de Services Essentiels

1) Notion et champ d'application

229. L'article 4 définit dans son quatrième alinéa la notion d'opérateur de services essentiels. Les OSE répondent aux critères prévus par l'article 5 paragraphe 2 de la même directive. Ainsi, est qualifiée d'OSE une entité publique ou privée répondant à ces 3 conditions cumulatives :

- Une entité fournissant un service essentiel au maintien d'activités sociétales et/ou économiques critiques ;
- La nécessité d'utiliser les réseaux et systèmes d'informations pour fournir ledit service
- Le fait qu'un incident ait « un effet disruptif important » sur la fourniture du service concerné.

230. Cette notion d'effet disruptif est précisément détaillée dans l'article 6 de la directive. En effet, pour déterminer l'importance d'un effet disruptif, six paramètres sont à prendre en compte par les Etats membres :

231. -le nombre d'utilisateurs liés au service fourni par l'entité concernée ; la dépendance des autres secteurs visés à l'annexe II à l'égard du service fourni par cette entité, les effets de l'incident sur les fonctions économiques, sociétales ou sur la sûreté

publique ; la part de marché de l'entité ; la portée géographique de l'incident ; l'importance de l'entité au regard du service qu'elle fournit, ce afin d'envisager la possibilité de solutions alternatives pour la fourniture du service.

232. Enfin l'incident est défini comme « tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information ».

233. En outre, l'article 4 effectue un renvoi à l'annexe II de la même directive qui définit les entités publiques ou privées qualifiées d'OSE.

234. Ainsi sont qualifiées d'OSE les entités suivantes :

- Les sociétés de transport terrestre, maritime et côtier de passagers et de fret, à l'exclusion des navires exploités à titre individuel par ces sociétés. La définition précise de ces entreprises se trouve dans l'annexe I du règlement 725/2004[3].
- Les entités gestionnaires des ports, les installations portuaires, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports. Un renvoi est ici effectué à la directive 2005/65/CE[4] en son article 3. Sont ainsi des OSE les ports, les interfaces navire/port, les installations portuaires, les points de contact pour la sûreté portuaire, et les autorités portuaires. Les installations portuaires sont finalement définies dans le règlement n°725/2004 précité : il s'agit d'« emplacements où a lieu l'interface navire/port ; elles comprennent les zones telles que les zones de mouillage, les postes d'attente et leurs abords à partir de la mer, selon le cas »
- Les exploitants de services de trafic maritime.

235. De surcroit les considérants 10 et 11 de la directive disposent que " dans le secteur des transports par voie d'eau, les exigences en matière de sécurité imposées par des actes

juridiques de l'Union aux compagnies, aux navires, aux installations portuaires, aux ports et aux services de gestion du trafic maritime portent sur l'ensemble des activités, y compris les systèmes de radio et de télécommunications, les systèmes informatiques et les réseaux. Une partie des procédures auxquelles il est obligatoire de se conformer concerne le signalement de tous les incidents et devrait donc être considérée comme une lex specialis, dans la mesure où ces exigences sont au moins équivalentes aux dispositions correspondantes de la présente directive.

236. Lors de l'identification des opérateurs dans le secteur des transports par voie d'eau, les États membres devraient prendre en compte les codes internationaux et les lignes directrices existants et futurs élaborés notamment par l'Organisation maritime internationale, en vue d'offrir une approche cohérente aux différents opérateurs maritimes."

2) Contrôle des Opérateurs de services essentiels par les Etats membres

a) Le principe du contrôle par l'Etat membre

237. Il résulte de l'article 14 de la directive que les Etats membres effectuent un contrôle sur les OSE sur trois aspects fondamentaux.

238. Tout d'abord, les Etats membres vérifient que les OSE adoptent des mesures techniques et organisationnelles pour une gestion des risques menaçant la sécurité des

réseaux et des systèmes d'informations. L'objectif est de fournir un niveau de sécurité suffisant au vu des risques existants.

239. Ensuite, les Etats membres s'assurent que les OSE effectuent les procédures nécessaires en vue de prévenir les incidents, afin que la continuité de leurs services ne soit pas impactée.

240. Enfin, les Etats membres veillent à la notification par les OSE des incidents ayant un impact substantiel sur la continuité des services essentiels qu'ils fournissent.

241. L'évaluation de l'ampleur de l'impact d'un incident prend en compte le nombre d'utilisateurs touchés par la perturbation du service essentiel ; la durée de l'incident ; et la portée géographique eu égard à la zone touchée par l'incident.

242. Les incidents subis par les OSE seront également reportés par les CSIRT non seulement aux autres Etats Membres de l'Union Européenne, mais aussi au public, si sa sensibilisation est nécessaire pour la gestion ou la prévention d'un incident en cours.

b) La délégation de compétences

243. Il résulte de l'article 15 que la directive met en place plusieurs compétences déléguées par les Etats Membres aux autorités compétentes afin d'encadrer les OSE.

244. Ainsi, les autorités compétentes peuvent premièrement exiger des OSE les informations nécessaires pour évaluer la sécurité de leurs réseaux et leurs systèmes d'informations. Puis elles peuvent demander les éléments qui prouvent la mise en exécution des politiques de sécurité. Si cette politique de sécurité est concrétisée par un audit effectué par un auditeur qualifié, les OSE doivent mettre les résultats et les

éléments probants à disposition de l'autorité compétente. Cette dernière doit toutefois notifier à l'OSE la finalité de la demande, ainsi que les informations exigées.

245. A la suite de l'évaluation, des instructions contraignantes peuvent être données par les autorités compétentes.

D) Groupe de coopération

246. Il faut ici se référer à l'article 11 de la directive.

247. L'objectif du groupe est la facilitation de la coopération entre les Etats membres, il est « de renforcer la confiance et de parvenir à un niveau élevé commun de la sécurité des réseaux et des systèmes d'informations », définie dans l'article 4 de la façon suivante : « La sécurité des réseaux et systèmes d'information consiste en leur capacité de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles. »

248. Ce groupe organise la mise en exécution des objectifs prévus par la directive. En effet, sont fournies des orientations stratégiques pour le fonctionnement du réseau des CSIRT. Le groupe s'occupe également de rendre la procédure de notification des incidents la plus efficace possible grâce à l'échange des bonnes pratiques à ce sujet.

249. Par ailleurs, en coopération avec l'ENISA, le groupe échange sur les bonnes pratiques quant à l'identification des opérateurs de services essentiels. La Commission adopte les actes fixant les modalités de fonctionnement du groupe de coopération.

Section II Le droit français

250. Il faut en tout premier lieu se référer au Livre Blanc sur la Défense et la Sécurité Nationale en date de 2008, qui avait été présenté à plus de 3500 militaires, policiers, et acteurs civils de la sécurité.

251. Dans la troisième partie de ce livre blanc, il est fait mention d'un objectif, celui de la protection des informations sensibles. (p. 182-183).

252. Il y est affirmé en préambule, que la France devra se pourvoir d'une capacité de défense de ses systèmes d'information. Cette menace est en effet considérée comme croissante. Par conséquence, cette défense devra être réactive et être mise en place à court terme.

253. Outre la mise en place de "produits de sécurité", des "réseaux de confiance" devront être élaborés afin de prévenir les menaces.

254. Par ailleurs, il est prévu une surveillance par les opérateurs de communication électronique. Il incombe à ces derniers de mettre en œuvre certaines mesures afin de protéger leurs réseaux contre les plus graves attaques.

255. Finalement, est prévue la création d'une agence chargée de la sécurité des systèmes d'information. Il est préconisé que celle-ci soit sous l'autorité hiérarchique du Premier Ministre, ainsi que sous la tutelle du Secrétariat Général de la Défense et de la Sécurité Nationale qui ne sera plus titulaire à proprement parler de l'exécution de la sécurité des systèmes d'information, mais plutôt de sa supervision.

256. Le livre Blanc préconise 4 missions pour cette agence.

257. Tout d'abord, le reprise et le renforcement des effectifs et moyens du SGDN alloués à la sécurisation des systèmes d'information.

258. Ensuite, la mise en place d'une compétence, centralisée par cette agence, de détection et de défense face à l'ensemble des attaques informatiques.

259. Puis, dans l'objectif de protéger les réseaux et systèmes les plus critiques de l'Etat, l'agence sera habilitée à recevoir les moyens nécessaires pour faire développer et acquérir des produits de sécurité essentiels. Ces derniers seront affectés à la protection des réseaux et systèmes critiques susmentionnés.

260. Finalement, elle conseillera le secteur privé, notamment les entreprises vouées à des activités d'importance vitale. Pour ce faire, il incombe notamment à l'agence de développer des sites Internet accessibles à tous.

261. L'exécution de ces recommandations s'est traduite par l'adoption du décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé "Agence Nationale de la Sécurité des Systèmes d'Information".

262. Il s'agit d'un service à compétence nationale.

I La Loi n°2018-133

263. -La loi n° 2018-133 du 26 février 2018, transpose la directive (UE) 2016/1148 du 6 juillet 2016 (NIS) qui vise à « assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'Information dans l'Union » (PE et Cons. UE, dir. (UE) 2016/1148, 6 juillet 2016, art.1,1) Cette directive met en place un cadre européen indispensable en présence d'activités transfrontalières interdépendantes. Elle fait corps avec le Règlement Général de la Protection des Données Personnelles (27 avril 2016) et la protection des informations commerciales non divulguées (Dir. (UE) 2016/943 du 8

juin 2016), deux textes également transposés en droit français, formant ce qui a été nommé « le printemps européen des données ».

264. Elle se réfère pleinement aux codes nationaux. Ainsi, L'article 1 er de la loi de la transposition effectue en premier lieu un renvoi à l'article L32 du Code des communications et des postes électroniques pour définir la notion de réseau et de systèmes d'informations. Par conséquent, est un réseau et système d'information tout réseau de communication, qui est défini par l'article susmentionné comme « toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage.

265. Cependant la loi française ne transpose que certains aspects de la directive NIS, se cantonnant à poser des exigences « en matière de sécurité, (prise au sens de la Directive, article 1, alinéa 3, citée plus haut) et de notification pour les opérateurs de services essentiels (OSE) et pour les fournisseurs de services numériques (FSN) » (PE et Cons. UE, dir. (UE) 2016/1148, 6 juill. 2016, art. 1, § 2 d), catégories qu'elle définit dans le droit français. Elle vise les réseaux de communication qui assurent un traitement automatisé de données. D'autres aspects de la Directive, concernant la stratégie Nationale de chaque état membre, sont confiés en France au pouvoir réglementaire, par exemple la création de l'Agence Nationale de Sécurité des Systèmes Informatiques

266. Ainsi, le champ de la loi n'est pas sans limite. Ses dispositions ne s'appliquent pas aux fournisseurs de réseaux et services de communications électroniques et aux prestataires de service de confiance déjà soumis à des exigences sécuritaires, ni aux secteurs déjà équipés d'un niveau de garantie équivalent. La protection des données personnelles s'appliquera cumulativement à ces dispositions.

A - La reconnaissance juridique de nouvelles entités.

267. La loi crée d'abord la catégorie d'Opérateur de Service Essentiel au fonctionnement de la société et de l'économie, au moyen de réseaux et de systèmes d'information à la continuité indispensable. Dans les secteurs listés en annexe du Décret 2018-384, les ministres désignent les opérateurs œuvrant dans leur domaine de compétence, acteurs les plus divers (fournisseurs d'eau, d'énergie, hôpitaux…)

268. Quant aux Opérateurs d'Importance Vitale pour la Nation, définis en France depuis la loi du 12 décembre 2005, ils sont paradoxalement exclus du champ d'application des OSE dont ils devraient par nature relever, et dont ils ont inspiré la définition[40], car ils étaient déjà soumis par le législateur français à un régime plus exigeant depuis la loi du 18 décembre 2013 : les O.I.V gèrent des établissements « dont l'indisponibilité obérerait gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou risquerait de mettre gravement en cause la santé ou la vie de la population » (article R. 1332-1 du code de la défense). Il n'était donc pas prévu qu'ils bénéficient du régime de coopération européen prévu pour les OSE à la suite d'un incident de sécurité.

269. La loi définit de manière plus limitative que la NIS les Fournisseurs de Service numériques, « tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle », c'est à dire à ses termes les « places de marché en ligne », « les moteurs de recherche » et les « services informatiques en nuage » (art. 10). Si les GAFAM extra-européens sont soumis à l'obligation d'avoir un représentant sur le territoire national, au cas où ils n'auraient pas de représentant ailleurs dans l'union, la loi écarte de ses exigences les petits FSN, pour des raisons

[40] V. en ce sens : DE MAISON ROUGE, O. Transposition de la directive NIS- de la Cybersécurité à la Cyber résilience. *Dalloz IP/IT.* pp. p.374.

économiques. Elle s'applique donc partiellement aux Fournisseurs de Services numériques.

B - Les obligations des nouveaux acteurs

270. Le régime appliqué à ces nouveaux acteurs est légèrement différencié. Présentant un risque fort, les OSE sont soumis à des règles strictes. Présentant des risques moindres, et œuvrant de part et d'autre des frontières, les FSN seront soumis à des règles plus souples, mais plus harmonisées (PE et Cons. UE, dir. (UE) 2016/1148, 6 juill. 2016, cons. 49).

271. Obligées d'identifier les risques par une analyse d'impact, les instances ainsi définies doivent prendre les mesures précisées par le pouvoir réglementaire, destinées à prévenir les incidents de sécurité ou à limiter leur impact.

272. Les OSE et les FSN sont tenus de déclarer les incidents survenus, et, seulement pour les graves, de les notifier, pour éviter la surcharge de l'ANSSI (art. 7 et 13). Ils doivent bien entendu en tenir registre et prendre en compte différents critères précis pour en évaluer la gravité (art. 13, I). Ainsi, les fournisseurs de service numérique mentionnés à l'article 11 déclarent, « sans délai après en avoir pris connaissance, à l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne, lorsque les informations dont ils disposent font apparaître que ces incidents ont un impact significatif sur la fourniture de ces services, compte tenu notamment du nombre d'utilisateurs touchés par l'incident, de sa durée, de sa portée géographique, de la gravité de la perturbation du fonctionnement du service et de l'ampleur de son impact sur le fonctionnement de la société ou de l'économie ».

273. Mais l'information du public n'intervient que si elle est nécessaire pour prévenir ou traiter un incident ou pour un motif d'intérêt général. C'est l'ANSSI qui est juge de l'opportunité et de l'étendue de cette information communiquée au public ou aux partenaires européens, c'est elle qui l'assure ou contraint les FSN à l'effectuer. (art. 3, II)

C - les contrôles et les sanctions

274. Le Premier ministre prend l'initiative des contrôles, d'office, n'importe quand pour les OSE (art.8), seulement a la suite du non-respect des exigences de sécurité ou de communications pour les FSN (art.14). L'ANSSI effectue ou fait effectuer ces contrôles de manière confidentielle à la charge des intéressés avant d'éventuelles sanctions (art. 4, 8, 9, 14 et 15E

275. Si certains déplorent les limitations dans le champ d'application de la loi, elle aura des incidences dans le comportement des acteurs et entre les acteurs, car elle crée de nouveaux devoirs, de nouvelles responsabilités de nature administrative ou civile[41]. Elle pose le problème de la validité des clauses élusives ou limitatives de responsabilités, de l'évaluation des préjudices immatériels, elle suscite de nouvelles obligations de transparence, de coopération, et de nécessaires adaptations dans le champ de l'assurance.

II - La catégorie restreinte des opérateurs d'importance vitale

276. Comme il a été vu précédemment, les Opérateurs de Services Essentiels bénéficient d'une certaine protection aux termes de la directive NIS. Toutefois, avant la transposition de cette dernière, le droit français avait déjà consacré une protection de

[41] DOUVILLE, T. Cybersécurité : transposition de la directive NIS, ses limites et ses conséquences. *La Semaine Juridique Edition Entreprise et Affaires.* 12 avril 2018, vol. 15-16, n°act. 284.

certains acteurs de l'industrie maritime. Cependant, comme nous allons le voir, le champ d'application de cette loi est plus restreint que celle de l'Union Européenne.

277. Tout d'abord, à l'issue des attentats du 11 septembre 2001, la France avait commencé une réflexion sur la notion même d'infrastructures critiques afin de pouvoir adapter au mieux la protection des entités qui seraient qualifiées comme telles.

A - La qualification de la notion

278. Une réponse arrive avec le Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale. En effet, l'article 2 définit la notion de secteur d'Activité d'Importance Vitale. Un tel secteur se constitue d'activités concourant à un même objectif. De surcroît, ces activités ont trait à la sécurité de la nation et à l'exercice de l'autorité de l'Etat, mais aussi, à la satisfaction des besoins essentiels pour la vie des populations et la production de biens et services indispensables.

279. Les opérateurs qui exercent des activités d'un secteur d'importance vitale se voient attribuer la qualification d'opérateurs d'importance vitale. Ces opérateurs gèrent ou utilisent au titre de ces activités des établissements, des ouvrages, ou des installations. Le dommage, l'indisponibilité, la destruction de ces derniers notamment en cas d'attaque[42] risquerait, soit d'accabler le potentiel économique, la sécurité ou la capacité de survie de la nation, ou de mettre en cause la santé ou la vie de la population. La liste des Opérateurs d'Importance Vitale est classée confidentielle pour des raisons de sécurité Nationale.

Par ailleurs, le décret donne une seconde définition de la notion d'opérateurs d'importance vitale. Il s'agit notamment des "opérateurs publics ou privés exploitant des

[42] "'un acte de malveillance, de sabotage ou de terrorisme"

établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation"[43].

280. Puis, par un arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, le Premier Ministre inclut dans ce secteur notamment le domaine des transports ainsi que les activités civiles de l'Etat.

B - Des protections et des exigences

281. La définition des opérateurs d'importance vitale a engendré leur prise en compte dans le Livre Blanc sur la Défense et la Sécurité Nationale en 2013. La lutte contre la cybermenace y est incluse au sein des moyens de prévention et de gestion des crises sur le territoire national. En effet, la protection contre les attaques informatiques, leur détection et l'identification de leurs auteurs sont considérées comme un élément de la souveraineté nationale. A ce titre, le renforcement de la sécurité des Systèmes d'Information de l'Etat est préconisé. Il est également prévu que les activités d'importance vitale au fonctionnement normal de la Nation soient soumises à des standards de sécurité à respecter. L'Etat veillera à la mise en exécution de ces standards, notamment dans ce qui a trait à la notification des incidents et des pouvoirs reconnus à l'Agence Nationale de la sécurité des Systèmes d'Information. Enfin, en réponse aux agressions informatiques, il est considéré nécessaire de mettre en place "une posture robuste et résiliente"[44] de protection des systèmes d'Information des opérateurs d'importance vitale.

[43] Article 1332-1 du Code de la défense

[44] Livre Blanc sur la défense et la sécurité nationale. Direction générale des relations internationales et de la stratégie, 2013. 106

282. La prise en compte de ces recommandations interviendra avec la 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.

283. L'article 21 de cette loi insère dans le Code de la défense l'article L2321-1. Le premier donne compétence au Premier Ministre pour définir et coordonner la politique relative à la sécurité et la défense des systèmes d'information.

284. L'article 22 quant à lui met en place plusieurs obligations à destination des opérateurs d'importance vitale qui sont relatives à leurs systèmes d'information.

285. Sur le plan de la protection des systèmes d'informations, l'article L1332-6-1 du Code de la Défense dispose que "Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais". Ces opérateurs sont en outre obligés d'informer le Premier Ministre d'une attaque subie, au terme de l'article L1332-6-2.

286. De surcroît, les opérateurs sont contraints de soumettre leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité prévues à l'article L. 1332-6-1. Ces contrôles sont effectués soit par l'autorité nationale des systèmes d'Information, soit par les services de l'Etat désignés par le Premier Ministre.

CHAPITRE 2- LE DROIT POSITIF APPLICABLE À LA CYBERSÉCURITÉ DANS L'INDUSTRIE MARITIME

287. Comme on a pu le voir, la création des notions d'Opérateurs de Services Essentiels et d'Opérateurs d'Importance Vitale permettent la création d'un droit commun de la cybersécurité.

288. En France, leur contrôle est effectué par l'Agence Nationale de la Sécurité des Systèmes d'Information.

PARTIE II LES INSUFFISANCES DANS LA MISE EN ŒUVRE DE LA PROTECTION CONTRE LA CYBERCRIMINALITÉ DANS L'INDUSTRIE MARITIME

TITRE I LES INSUFFISANCES DANS L'EXÉCUTION DES PROTECTIONS TECHNIQUES ET JURIDIQUES CONTRE LA CYBERCRIMINALITÉ MARITIME

CHAPITRE 1- L'EXÉCUTION DE LA GESTION INTERNE DU RISQUE

289. Pour pousser les acteurs à se prémunir au mieux contre les pannes et contre la cybercriminalité, les instances officielles ont mis en place une démarche d'homologation de sécurité.

290. Sur ce point, il faut bien garder en tête que la cybersécurité s'est créée en 2000-2010. L'objectif était alors de sécuriser des Systèmes d'Informations fermés avec peu d'interfaces. On pouvait donc se concentrer au cœur du système considéré. Étaient principalement sécurisés l'intérieur et les passerelles.

291. Ce mode de fonctionnement est tout simplement impossible aujourd'hui. En effet, les Service numériques sont désormais connectés avec l'extérieur en permanence. On n'arrive donc plus à définir les frontières d'un système d'information.

292. On doit donc envisager l'écosystème, dont le rôle est mieux reconnu aujourd'hui qu'en 2017, lorsque l'auteur du mémoire précité critiquait sa faible prise en compte. On considère notamment la sécurité de la chaîne d'approvisionnement, celle des différentes parties prenantes à une activité numérique. Cet élément est absolument crucial. Comme l'attaquant tombe sur des systèmes d'informations mieux sécurisés, il va passer de plus en plus par l'écosystème.

293. A l'origine, le navire était un système clos.

294. Maintenant, le navire est connecté à Internet en permanence. On n'achète plus des systèmes mais des services, disponibles seulement si on est connecté à Internet.

295. Les activités, les systèmes vitaux du bateau, la propulsion, l'énergie électrique, le système de navigation sont connectés à Internet en permanence. On les utilise et on paie des services par rapport à l'utilisation qui en est faite. Par exemple, autrefois l'armateur achetait un générateur électrique à un fournisseur pour équiper son navire.

296. 87. Mais maintenant le fournisseur, par exemple Wartsila, installe à bord son propre matériel qui doit toujours être connecté, et vend de l'énergie à l'armateur responsable de l'entretien

297. Avec les systèmes d'information de navigation la situation est identique. Autrefois par exemple, l'armateur achetait le système de Visualisation des Cartes Électroniques et d'Information. Puis, par CD-ROM, lui étaient envoyées les cartes numériques signées par le fournisseur. L'armateur les téléchargeait sur le Système de Visualisation des Cartes Électroniques et d'Information. Maintenant, le système de navigation est connecté à la mer par Internet et les cartes de navigation sont mises à jour et téléversées depuis internet par le fournisseur du service. Si un 'adversaire a pris le contrôle des fournisseurs d'électricité ou du système de navigation de l'armateur, il est capable de prendre le contrôle du navire. Dans ce cas de figure, toutes les sécurisations opérées par l'armateur sont vaines.

298. Si le fournisseur du système de navigation, le fournisseur de la propulsion, le fournisseur de l'énergie électrique se fait attaquer par l'adversaire, il faut bien garder à l'esprit qu'ils demandent à l'armateur un accès depuis la terre au navire via Internet. Dès lors, si l'adversaire prend le contrôle sur l'un des fournisseurs, l'adversaire pourra pénétrer et attaquer n'importe quel système d'information.

299. Cela vaut aussi bien entendu et surtout pour les systèmes d'information installés à bord du navire. Le fournisseur du service de communication par satellite ne se contente pas en effet d'installer un canal. Il doit également mettre en place plusieurs autres fonctionnalités pour le S.I. à bord, qui gèrent la communication, la comptabilité, impliquent les paramètres du moteur, toutes informations qui transitent sur le réseau et peuvent être exploitées de manière malveillante par tout adversaire qui aurait investi le service de communication.

300. L'armateur est obligé de demander aux fournisseurs des garanties de sécurité. Il faut qu'il puisse avoir confiance en eux. Donc ce sera aux fournisseurs de donner des garanties sur la sécurité. L'armateur peut aussi bien se protéger contractuellement, auditer les différents fournisseurs, demander quelles garanties sont mises en place par le fournisseur. L'objectif pour l'armateur sera de ne pas être paralysé si l'un de ses fournisseurs se fait attaquer.

301. L'enjeu est donc d'assembler une chaîne de confiance entre l'armateur et tous les acteurs qui l'aident à mener son activité, et les bénéficiaires. Fort des garanties de sécurité présentées par les fournisseurs, l'armateur accordera les siennes à ses clients.

302. Et dans un écosystème global, tout le monde doit pouvoir donner des garanties de sécurité. En effet, l'adversaire est très susceptible d'attaquer le maillon faible de la chaîne. Si un des acteurs de la chaîne dispose d'un niveau médiocre de sécurité, il va être attaqué, l'adversaire aura donc accès à tous les maillons.

303. Avec la nouvelle méthode d'expression des besoins et identification des objectifs de sécurité produite par l'Agence Nationale de Sécurité des Systèmes d'information, ces paramètres sont pris en compte. Il faut bien comprendre que les normes précédentes ne sont pas abandonnées. D'autres processus y sont ajoutés. On s'intéresse à l'écosystème en lui-même.

304. C’est ce que permettent EBios Risk Manager, ainsi que l’homologation de sécurité. L’objectif est de mettre un décideur devant la réalité de ces risques, en lui faisant comprendre les risques du système et de l’écosystème. Ainsi, sa décision pourra être aussi avisée que possible.

Section I - L'homologation de sécurité

305. C'est à la fois pour les instances concernées une incitation à se garantir, et à terme une source de confiance pour leurs usagers ou leurs clients

I. Les étapes principales

306. Pour obtenir une homologation, un système doit avant tout être éligible.

Etape 1 : Quels systèmes convient-il d’homologuer et pourquoi ?

307. La réglementation définit les établissements susceptibles d'homologation

1) le référentiel réglementaire.

308. La démarche d’homologation peut être soit obligatoire, soit facultative. Elle est notamment rendue obligatoire par la politique de sécurité des systèmes d’information de l’Etat.

309. Au terme de la circulaire n° 5725/SG du Premier Ministre en date du 17 juillet 2014, cette politique de sécurité s’applique aux établissements publics sous tutelle d’un ministère. Par conséquent, les Grand Ports Maritimes sont soumis à cette réglementation.

310. Cette démarche est en outre conseillée depuis son existence par l'Agence Nationale de la Sécurité des Systèmes d'information.

2) le périmètre du système

311. Trois types d'éléments devront être pris en compte dans la perspective de l'homologation.

312. Tout d'abord, seront considérés des éléments fonctionnels et d'organisation, tels que les conditions d'emploi des produits de sécurité, les dispositifs de détection et de gestion des incidents et la gestion des droits. L'on parle ici de la gestion de l'accès d'un utilisateur à un certain type de fichier.

313. Puis, des éléments techniques devront être analysés. Il sera ici notamment question de l'architecture du système. Un élément fondamental devra alors être précisé : l'interconnexion du système considéré avec d'autres systèmes.

314. En effet, il est plausible que le système d'information considéré soit composé de matériel et de logiciels achetés à un éditeur, un industriel, une marque tierce. Dans ce cas de figure, la labellisation de ces logiciels est fondamentale du fait de leur rôle essentiel dans la mise en place de la sécurité.

315. Si le matériel est utilisé d'un point de vue opérationnel, un cahier de sécurité devra être demandé au fournisseur de ce matériel. Ce dernier liera le fournisseur par des garanties, des conditions d'emploi et des règles de sécurité qu'il aura lui-même édictées.

316. Finalement : devront être prises en compte les localisations géographiques et les caractéristiques des locaux.

Etape 2 : Quel type de démarche doit être mis en œuvre ?

317. Les instances soumises à l'homologation ou les candidats volontaires devront mettre en œuvre une démarche à la fois guidée et autonome.

1) Autodiagnostiquer les besoins de sécurité du système et le niveau de maturité SSI de l'organisme

318. A cette fin, deux outils sont mis à disposition par l'ANSSI, en annexes à son guide d'homologation. Le premier permet d'évaluer les besoins de sécurité des systèmes d'information. Il permet de déterminer à quel niveau le système a besoin de sécurité. Le second clarifie le niveau de maîtrise de l'organisation quant à la gestion de la sécurité des systèmes d'information. Ces deux annexes sont disponibles dans le cadre de ce mémoire (V. Annexe)

2) Choisir la démarche appropriée

319. Grâce à ces diagnostics, l'organisation détermine la démarche d'homologation appropriée à son cas. Il faut agir de manière avisée, car une démarche trop lourde ou trop légère aurait pour conséquence une incomplétude et une mise en danger du succès de l'homologation.

320. La démarche pourra être soit très légère (Pianissimo), faible-moyenne (mezzo piano), moyenne forte (mezzo forte) ou forte, pour employer des métaphores musicales.

321. Dans le premier cas la démarche sera autonome et minimale. La seule aide reçue par l'autorité d'homologation sera issue de ses ressources internes ou du guide de l'homologation.

322. Dans le second cas, la démarche sera plus approfondie.

323. Dans le troisième cas, la démarche assistée sera menée par l'autorité d'homologation avec l'aide d'un conseil externe, en complément des indications du guide commenté.

324. Dans le quatrième cas, l'organisme dispose déjà d'un niveau de maturité suffisant. Dès lors l'autorité d'homologation est dispensée d'avoir recours à ce guide.

Etape 3 : Qui contribue à la démarche ?

325. La troisième étape porte sur la désignation des personnes qui seront intégrées au processus d'homologation. Sont prévus l'autorité d'homologation, la commission d'homologation, puis les différents acteurs de l'homologation.

1) L'autorité d'homologation

326. Il s'agit de la personne qui, à l'issue de l'instruction du dossier d'homologation, prononcera l'homologation de sécurité du système d'information. Par cette action, l'autorité d'homologation accepte les risques identifiés sur le système.

327. L'autorité d'homologation désignée devra en outre disposer de compétences étendues pour pouvoir assumer l'ensemble des responsabilités prises à l'issue de l'homologation.

328. Cette autorité désignera le responsable du processus d'homologation. Ce dernier mènera le projet de l'homologation au nom de l'autorité.

2) La commission d'homologation

329. La commission assiste l'autorité d'homologation dans l'instruction de cette dernière.

330. La commission prépare la décision de l'homologation. Elle suit la planification du processus de l'homologation, mais procède surtout à l'analyse de l'ensemble des documents communiqués lors de la procédure.

3) Les acteurs de l'homologation

331. La maîtrise d'ouvrage représente les différents métiers et postes.

332. Elle s'assure de la prise en compte des contraintes liées à l'utilisation du système d'information.

a) Le Responsable de la sécurité des systèmes d'information

333. Si l'organisation dispose d'un responsable, ce dernier est susceptible d'être désigné responsable du processus d'homologation. Si tel n'est pas le cas, il pourra être secrétaire de la commission d'homologation, ou membre de cette dernière.

b) Le responsable d'exploitation du système

334. Cette entité remplit un rôle opérationnel. Au quotidien, c'est elle qui est responsable de l'exploitation du système d'information

c) Les prestataires

335. Ces derniers peuvent être intégrés dans la commission, ou simplement consultés. Ils assistent et produisent des éléments qui seront versés au dossier d'homologation, et répondent aux questions de la commission d'homologation.

336. Certains prestataires de l'ANSSI jouent un rôle fondamental : celui de la vérification de la solidité et de la sécurité du système d'information. Dans ce sens, les Prestataires d'Audit de la Sécurité des Systèmes d'Information, peuvent être contactés par les organisations pour effectuer des attaques sur leurs systèmes d'information. A l'issue de ces attaques, un rapport sera émis avec des recommandations à destination de l'organisation. Dans le cas du Grand Port Maritime de Marseille, ces recommandations sont systématiquement suivies afin d'assurer la pérennité de sa cybersécurité[45].

d) Les systèmes interconnectés

337. Ces derniers peuvent être associés à l'homologation du système de l'organisation lorsque le système homologué a un impact sur leurs systèmes. Ils peuvent en outre émettre des avis et des certificats concernant le système. Cette émission est importante dans la chaîne de confiance entre les différents opérateurs d'une même chaîne de production. En effet, elle permet d'offrir des garanties aux utilisateurs finaux du service. Si par exemple, l'armateur s'est vu accorder par un fournisseur de diésel électrique des garanties quant à la sécurité, il pourra à son tour garantir à un client que son système est sécurisé.

Etape 4 : Comment s'organise-t-on pour recueillir et présenter les informations ?

1) Le contenu du dossier d'homologation

338. L'on pourra notamment y retrouver l'analyse de risques, la politique de sécurité du système d'information, la cartographie des systèmes d'information de l'organisme, ainsi que les décisions d'homologation des systèmes interconnectés.

[45] [audio]. Entretien avec Paul Franquart. 11 mai 2020.

339. Le contenu sera proportionnel à la démarche précédemment adoptée.

2) Le planning

340. A l'issue de l'homologation, sera effectuée la mise en service opérationnelle. Par conséquent la planification de l'homologation devra être préalablement établie.

341. Dans ce planning, seront déterminées les différentes tâches aux différents acteurs de l'homologation précitée.

Etape 5 : La maîtrise des risques : quels risques pèsent sur le système ?

1 L'analyse de risques

342. Selon l'ANSSI, un risque est la combinaison de deux éléments : un évènement redouté et un scénario de menaces[46]. Le niveau du risque quant à lui est mesuré en fonction de son impact potentiel et de sa vraisemblance.

343. L'analyse des risques dépendra de la démarche adoptée suite à l'auto-diagnostic.

344. SI la démarche pianissimo est adoptée, l'organisation devra établir la liste des menaces potentielles susceptibles de se réaliser. Ces menaces sont présentes dans l'annexe 4. Ensuite, l'organisation devra déterminer les biens essentiels susceptibles d'être affectés. Pour obtenir un scénario de risques, l'organisation devra décrire l'impact de la menace sur la disponibilité, l'intégrité ou la confidentialité du bien essentiel.

345. Si la démarche Mezzo Piano ou Mezzo Forte est adoptée, une analyse de risques approfondie sera alors grandement conseillée. Pourra ici être utilisée la Méthode

[46] EBIOS : la méthode de gestion des risques SSI Un outil simple et puissant. 2010. Disponible à l'adresse : https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-PlaquetteMetho-2010-04-081.pdf

d'Expression des Besoins et Identifications des Objectifs de Sécurité (EBIOS), mise à disposition par l'Agence Nationale de la sécurité des Systèmes d'information. Ce Système permet d'établir une Fiche d'expression Rationnelle des Objectifs de sécurité.

346. Après avoir déterminé les risques susceptibles d'entrer dans le champ d'application du système homologué, il faut déterminer les mécanismes permettant de contenir ces derniers. A la suite de l'application des mesures, des risques résiduels peuvent subsister. Ces derniers devront être acceptés.

347. Si la démarche choisie est la démarche pianissimo, le minimum requis devra être appliqué. Il faudra alors se référer aux différents guides de l'Agence Nationale de la Sécurité des Systèmes d'Information, notamment celui relatif aux 40 règles d'hygiène informatique.

348. Si la démarche choisie est la démarche Mezzo Piano ou Mezzo Forte, les risques considérables trouveront leur protection grâce à la méthode EBIOS.

Etape 6 : La réalité correspond-elle à l'analyse ?

349. Il sera ici procédé à l'évaluation de l'écart entre l'évaluation du risque et la réalité de ce dernier. Cette évaluation pourra être effectuée à n'importe quel moment du cycle de vie du système.

1) Réalisation du contrôle

350. Pour la démarche pianissimo, l'audit sera optionnel.

351. Pour la démarche piano, un audit sera conseillé sur les éléments les moins maîtrisés du système.

352. Pour la démarche Mezzo Forte, un audit en conformité avec les exigences des prestataires d'audit de la sécurité des systèmes d'information sera conseillé.

353. Finalement, le périmètre du système contrôlé devra être délimité par l'autorité d'homologation. Des tests d'intrusion pourront également être effectués.

354. Comme indiqué précédemment, les Prestataires d'Audit de la Sécurité des Systèmes d'Information procèdent à la vérification de la solidité et de la sécurité du système d'information.

2) Conséquence de l'audit sur le dossier

355. L'écrit est nécessaire pour le contrôle de sécurité. Si la démarche choisie est la Mezzo Forte ou la Mezzo Piano, un rapport sera rédigé. Ce dernier mettra en relief l'évolution des menaces sur le système, la découverte de nouvelles vulnérabilités, le conseil de nouvelles mesures correctives.

Etape 7 : Quelles sont les mesures de sécurité à mettre en œuvre pour couvrir ces risques ?

1) Le traitement du risque

356. A l'issue des étapes précédentes, certains risques ne seront pas couverts par les mesures mises en place. Pour tout ou partie de chaque risque, quatre options pourront être choisies.

357. Premièrement le risque pourra être évité : ici, il s'agira de supprimer la circonstance ou la situation génératrice de risque. D'un point de vue opérationnel, cette option semble compliquée à mettre en œuvre.

358. Une seconde option consistera à réduire le risque, ce qui consistera à adopter des mesures pour réduire la vraisemblance et/ou l'impact du risque.

359. Le risque pourra troisièmement être assumé. Les conséquences éventuelles seront acceptées sans mettre en place de mesures supplémentaires.

360. Les risques pourront être finalement transférés, ce qui consiste à en faire assumer la responsabilité à un tiers ou à partager les conséquences d'un sinistre.

361. Dans l'industrie maritime, les risques sont souvent assumés sans connaissance des conséquences de l'impact. En effet, la faiblesse ou l'inexistence du retour sur investissement pour le cyber, font que plusieurs risques sont acceptés, sans réelle prise en compte de leurs conséquences.

2) La mise en œuvre des mesures de sécurité

362. Ces mesures peuvent être techniques, organisationnelles ou juridiques. Elles sont décidées par l'autorité d'homologation.

363. S'il y a recours à un prestataire externe, les mesures de sécurité peuvent être mises en œuvre grâce à un contrat apportant la garantie de la protection des processus et données et accessibles par des utilisateurs légitimes (Lien avec Caparros condition de sécurité etc.)

3) Définition du plan d'action

364. Ce plan vise les risques résiduels ne pouvant être couverts par des mesures techniques ou organisationnelles. Y sont indiquées les vulnérabilités éventuelles, leur degré de gravité, ainsi que l'action envisageable pour contenir les risques afférents.

Etape 8 : Comment réaliser la décision d'homologation

365. Comme il a été expliqué précédemment, la décision d'homologation consiste en un acte par lequel le responsable d'une organisation atteste d'une part qu'une analyse de sécurité a été effectuée, d'autre part qu'elle a été prise en compte.

1) Le périmètre de l'homologation

366. Plusieurs éléments sont à prendre en compte dans ce cadre.

367. Tout d'abord, comme il a été noté précédemment, l'évaluation des Grands Ports Maritimes, soumis à la Politique de Sécurité des Systèmes d'information de l'Etat, est obligatoire. Ensuite, devront être considérées les pièces versées au dossier d'homologation. Enfin, il conviendra de prêter attention à trois périmètres.

368. Le premier sera le périmètre géographique et physique.

369. Le second sera le périmètre fonctionnel et organisationnel. Il s'agira notamment de l'inventaire des informations traitées par le système et les différents types d'utilisateurs.

370. Le troisième portera sur le périmètre technique. Il s'agira ici des prestataires, de l'architecture et de la cartographie des différents systèmes.

371. Finalement, en fonction des risques résiduels identifiés, l'autorité prononçant l'homologation peut assortir cette dernière de conditions d'exploitation mais aussi de plans d'action afin de maintenir le niveau de sécurité du système d'information.

2) La durée de l'homologation

372. Pour un système courant peu de risques, l'homologation pourra durer cinq ans. Dans le cas contraire, la durée de l'homologation sera comprise entre 1 et 3 ans.

373. La détermination de cette durée dépendra notamment de l'exposition du système à de nouvelles menaces.

3) Condition de suspension ou de retrait de l'homologation

374. L'homologation ne demeure valide que dans un contexte précisément déterminé. Si ce dernier change, le dossier d'homologation devra être réexaminé, ou retiré. Les circonstances suivantes permettent notamment de qualifier un changement de circonstances :

375. -changement d'homologation des autres systèmes interconnectés

376. -changement d'un ou plusieurs prestataires

377. -changement du niveau du risque

378. Dès lors, il est pertinent que la commission d'homologation se réunisse annuellement pour examiner si les objectifs de l'homologation sont respectés.

379. Finalement, si la mise en service opérationnelle d'un système est nécessaire malgré une présence de risques résiduels rendant l'homologation impossible, une autorisation provisoire d'emploi avec un encadrement précis pourra être prononcée.

Etape 9 : Qu'est-il prévu pour maintenir la sécurité et continuer de l'aménager ?

1) Suivi de l'homologation

380. Ce suivi annuel consiste en une mise à jour du dossier et une analyse des incidents et des évolutions qui ont eu lieu. Il est complété par des analyses de vulnérabilité. Enfin, il est pertinent de réunir périodiquement la commission d'homologation. En effet, cela permet une vérification du respect des critères, et, in fine, des conditions d'homologation. Ces réunions périodiques ont pour avantage de ne pas avoir à initier depuis le début le processus de l'homologation lorsqu'elle arrive à son terme.

2) Maintien en condition de sécurité

381. L'entité en charge du maintien du dossier d'homologation doit mettre en place une veille permettant de corriger les failles qui apparaissent dans le système afin qu'elles soient corrigées. Cette veille est absolument fondamentale dans la mise en place d'une protection agile contre la cybercriminalité. En effet, les failles sont constamment recherchées par les adversaires. Dès lors, la recherche des vulnérabilités permet de mieux appréhender les systèmes de défense face aux attaques. C'est ce à quoi servent par ailleurs les clauses de sécurité et de maintien en condition de sécurité du système. Celles-ci pourront être vérifiées grâce au guide d'externalisation de l'ANSSI.

382. Si longue est précautionneuse, entourée de garantie que soit la procédure d'homologation, elle ne vient pas à bout des risques issus des défaillances du système, des attaques extérieures. Elle mobilise pourtant un outil précieux, la méthode Ebios d'expression des besoins et indentification des besoins et objectifs de sécurité.

II. L'expression des besoins et identifications des objectifs de sécurité

383. L'EBIOS Risk Manager est une méthode d'appréciation et de traitement des risques numériques. Elle permet une appréciation des risques d'ordre numérique en commençant par une acception générale du risque pour aller vers une acception particulière.

384. L'on entend par acception générale l'étude des grands objectifs du système étudié. Par conséquent, seront d'abord pris en compte les principes de base et les cadres du droit positif. Puis, l'acception spéciale prendra en compte quant à elle les scénarios spécifiques susceptibles de se réaliser. La première étape sera celle de l'évaluation de la conformité du système à ce que l'on pourrait appeler l'état de l'art. L'évaluation des scénarios quant à elle visera de manière plus ciblée les situations qui auraient pour point de départ des menaces intentionnelles.

385. Cette démarche implique le concours de cinq ateliers : Le cadrage et le socle de sécurité, les sources de risques, les scénarios stratégiques, les scénarios opérationnels et le traitement du risque.

386. Le premier atelier prend en compte les deux piliers généraux précités, à savoir les principes de base et le cadre du droit positif. Les ateliers 2,3 et 4 se concentrent quant à eux sur l'approche des scénarios susceptibles de concrétisation.

387. Le dernier atelier porte quant à lui sur le traitement pratique du risque.

1) Cadrage et Socle de Sécurité

388. Au sein d'une organisation, la direction, les métiers, les Responsables de Sécurité des systèmes d'information et la Direction des Systèmes d'Information pourront participer à ce premier atelier.

a) le cadre de l'étude

389. Seront d'abord définis les objectifs de l'étude.

390. Ils pourront notamment être l'homologation du système d'information, ou alors le niveau de sécurité à atteindre pour bénéficier d'une certification produit.

391. Puis, les participants à l'étude seront identifiés

b) périmètre métier et technique

392. Les missions, valeurs métiers et objets d'études seront ici recensés. Les valeurs métiers correspondent aux informations ou processus jugés importants, qu'il conviendra de protéger. Il s'agit du patrimoine informationnel qu'un adversaire aurait intérêt à attaquer afin de parvenir à ses fins. Par exemple, si la mission étudiée est l'identification et la fabrication des vaccins, l'une des valeurs métiers sera la recherche et le développement.

393. Par ailleurs, un bien support sera présent pour exécuter une valeur métier. Dans le cas de la recherche et développement de vaccins, des serveurs bureautiques pourront stocker les données de recherche et développement.

c) identifications des évènements redoutés

394. Les évènements redoutés portent atteinte à la disponibilité, la traçabilité, l'intégrité, la confidentialité de la valeur métier considérée.

d) Détermination du socle de sécurité

395. A l'issue de cet atelier, plusieurs normes de base s'appliquant à l'objet d'études devront être désignées.

396. Il pourra notamment s'agir de la norme 27001 ou de recommandations de l'Agence Nationale pour la Sécurité des Systèmes d'Information.

2) Sources de risques

397. L'objectif est ici de déterminer les sources de risques ainsi que les objectifs visés. Les participants sont identiques à ceux de la première étape.

398. Les couples sources de risques/objectifs visés devront être évalués, puis hiérarchisés.

3) Scénarios Stratégiques

399. Participeront à cet atelier uniquement les métiers et les architectes fonctionnels. A l'issue de cet atelier, seront notamment déterminées les mesures de sécurité retenues pour l'écosystème, ainsi que la cartographie de menace numérique de l'écosystème et les parties prenantes critiques.

400. Cette notion d'écosystème est absolument fondamentale. Elle peut être définie comme l'ensemble des parties prenantes qui peuvent être en interaction avec le système d'information considéré. Dans le navire, il pourra s'agir du fournisseur de diésel électrique, qui demandera à l'armateur que son navire soit en permanence connecté afin que la fourniture du service soit opérationnelle. Dans le cas d'un laboratoire de recherche, il pourra notamment s'agir de fournisseurs Industriels de produits chimiques.

401. L’écosystème et sa connaissance sont essentiels pour une bonne cybersécurité. En effet, l’adversaire souhaite attaquer le maillon le plus faible d’une chaîne. Si l’attaquant parvient à pénétrer les logiciels de navigation, ou les cartes, l’utilisateur ne disposera plus d’aucun levier pour parer cette attaque.

402. Par conséquent, il sera nécessaire d’évaluer le niveau de menace induit par chaque partie prenante de l’écosystème sur l’objet étudié. Il sera ensuite possible d’établir la cartographie des menaces numériques de l’écosystème.

403. Puis, il faudra imaginer des scénarios plausibles et en déterminer le niveau de gravité.

404. Finalement, à l’issue de la mise en évidence des vulnérabilités liées aux parties prenantes, des mesures de sécurité seront à mettre en place.

4) Scénarios opérationnels

405. Participeront à cet atelier les RSSI, les DSI et éventuellement un spécialiste en cybersécurité.

406. Dans cette étape, des scénarios opérationnels seront imaginés, puis leur vraisemblance sera évaluée.

407. Dans l’imagination des scénarios opérationnels, les biens supports précédemment cités devront être identifiés. En effet, ces derniers peuvent constituer des vecteurs d’entrée ou un relais de propagation pour une attaque.

408. Puis les scénarios stratégiques d’attaque permettront de créer des schémas d’attaque.

409. Finalement, les scénarios opérationnels seront étudiés au regard de leur vraisemblance.

III L'externalisation

410. Si les acteurs tentent de mettre à niveau la sécurisation de leur système en œuvrant pour l'homologation, s'ils évaluent leurs besoins par l'Ebios, ils sont amenés à répondre à un autre défi de cybersécurité s'ils procèdent à l'externalisation de leur système d'information.

411. Le 3 décembre 2010, l'Agence Nationale de la Sécurité des Systèmes d'Information annonce la mise à disposition d'un guide relatif à l'externalisation[47] des systèmes d'informations.[48]. L'intérêt de ce guide est le suivant : « En externalisant un système d'information, on prend le risque de ne plus pouvoir le maîtriser ni protéger ses données. Il est donc indispensable de faire appel à des prestataires qui s'engagent sur la sécurité »[49].

412. Par la publication de ce guide, l'Agence Nationale de la sécurité des systèmes d'information permet aux entreprises et aux administrations de sécuriser leurs opérations d'externalisation.

413. Plusieurs risques sont encourus par l'armateur recourant à l'externalisation. En effet, le prestataire choisi peut tout d'abord recourir à un sous-traitant. Dans ce cas de

[47] Opération consistant à confier à un prestataire tiers à l'organisation tout ou partie d'une activité dont la gestion s'effectuait jusqu'alors en interne

[48] France, Agence Nationale de la Sécurité des Systèmes d'Informations, *Communiqué de Presse Externalisation, Cloud Computing : maîtriser les risques pour les systèmes d'information* en ligne. 3 décembre 2010.

[49] Olivier Ligneul, Chef du Bureau Conseil et assistance à l'Agence Nationale de la Sécurité des Systèmes d'Informations

figure, il sera nécessaire que le donneur d'ordre, par exemple l'armateur, accepte chacun des sous-traitants missionnés.

414. Par ailleurs, les choix techniques du prestataire sont susceptibles de souffrir de limitations en matière de sécurité. Cela peut notamment s'expliquer par des raisons économiques. Par conséquent, le prestataire devra démontrer la conformité de ses équipements vis-à-vis des différentes exigences de sécurité. Lorsque cette étape sera complétée, le donneur d'ordre sera apte à valider les différents choix du prestataire.

415. Compte tenu de ces différents risques, susceptibles de s'appliquer dans le cadre de l'industrie maritime, est préconisée par le guide l'élaboration d'un plan d'assurance de la sécurité. Il s'agit ici de l'ensemble des engagements pris par la personne soumissionnaire au donneur d'ordre pour garantir les exigences de sécurité de ce dernier.

416. Afin d'y parvenir, trois étapes préalables devront être exécutées.

417. Premièrement, une analyse des risques pesant sur le système d'information devra être effectuée. Cette étude permettra de déterminer les objectifs de sécurité, ce qui permettra de définir un cadre préalable au contrat conclu entre le donneur d'ordre et le titulaire.

418. Deuxièmement, le donneur d'ordre spécifiera grâce à la démarche précédente les exigences de sécurité ainsi que des clauses de sécurité. Ces éléments figureront dans un cahier des charges. Les candidats fourniront alors le plan d'assurance sécurité. Comme indiqué plus haut, ce document énumère les engagements pris par le futur prestataire afin d'être en conformité avec les exigences de sécurité du donneur d’ordre pendant toute la durée du contrat. De surcroît, la clause suivante devra affirmer l'engagement du prestataire à exécuter les obligations selon un plan d'assurance sécurité :

419. "Le titulaire s'engage à exécuter ses obligations en termes de sécurité des systèmes d'information selon le Plan d'Assurance Sécurité, dénommé PAS, décrit en annexe du contrat. Le titulaire est responsable de la rédaction initiale du PAS ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité du donneur d'ordres pendant toute la durée des prestations"[50].

420. Le document prévoit des clauses-types applicables au monde de l'industrie maritime. L'une d'entre elles permet au donneur d'ordre que les dispositions prises par le prestataire satisfassent à son exigence de sécurité.[51] La clause prévoit en outre la pratique de tests intrusifs. Ces tests seront prévus dans une charte commune signée par le prestataire, l'exécutant de l'audit et le client. Finalement, le client devra prévoir la possibilité d'avoir recours à l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

421. Puis une autre clause a trait aux obligations à mettre en œuvre par le prestataire :

422. "Le prestataire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer le client des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention. Outre le respect de ses obligations au titre de la convention de service, le prestataire informera préalablement le client de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système. Le prestataire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations. Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un

[50] Maîtriser les risques de l'infogérance/Externalisation des Systèmes d'Informations". Agence Nationale de la Sécurité des Systèmes d'Information, Décembre 2010.

[51] "Le client doit pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire".

protocole[52], une installation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse[53] et des capacités d'attaque par force brute[54] doivent être prises en compte".

423. Une obligation fondamentale dans cette clause est le maintien en conditions de sécurité. En effet, selon Fabien Caparros[55], un logiciel sérieux considéré dispose en son sein de l'état de l'art[56] en matière de sécurité informatique. Il faut ensuite paramétrer chaque système selon ses spécificités, puis le maintenir en conditions de sécurité, ce qui constitue un enjeu fondamental et potentiellement une source de vulnérabilité. Si les mises à jour de sécurité, par défaut d'organisation, ne sont pas effectuées dès qu'elles sont disponibles.

424. Cela passe par un contrat Logiciel. Par exemple, lors de l'achat d'un ordinateur, le client dispose de Windows. Contractuellement, Windows envoie des mises à jour de sécurité que l'utilisateur devra mettre en œuvre. Ce maintien en condition est prévu par une clause contractuelle qui prévoit le maintien des conditions de sécurité. En pratique, les différents fournisseurs envoient des mises à jour. Et ce sera au client, en l'occurrence à l'armateur de s'organiser pour les mettre en place.

425. Ainsi, l'inexécution de mises à jour envoyées par le fournisseur a pour conséquence que le système d'information reste exposé aux vulnérabilités non protégées.

[52] Ensemble de règles informatiques pour un type de communication en particulier.

[53] Discipline se spécialisant dans la déduction d'informations chiffrées sans clé de chiffrement

[54] Attaque se fondant sur l'essai de différentes combinations afin de pouvoir deviner le mot de passe d'un utilisateur

[55] CAPARROS, F. [audio]. 2 juillet 2020.

[56] Ensemble des connaissances et techniques disponibles dans un domaine considéré à un instant T.

426. Enfin, le donneur d'ordre dira si le Plan de sécurité est conforme au regard des exigences formulées. Dans l'affirmative, le Plan d'Assurance Sécurité sera annexé au contrat principal.

427. Force est donc de constater que l'Agence Nationale de la Sécurité des Systèmes d'Information met à disposition des entreprises et des administrations un guide complet quant à la démarche à adopter dans la gestion du risque cyber. L'entreprise qui exécute ces recommandations sera prémunie contre de nombreux risques susceptibles de réalisation au vu de sa situation particulière, et pourra être garantie vis-à-vis des prestataires qu'elle emploie. Toutefois, dans nombre de cas, ces recommandations sont exécutées d'une manière incomplète. Or, les éléments qui ne sont pas exécutés sont absolument cruciaux dans la protection de l'entreprise ou de l'administration considérée.

Section II- Les défaillances dans la mise en oeuvre

428. Comme nous l'avons vu précédemment, deux notions clés, les Opérateurs de Service Essentiels et les Opérateurs d'Importance Vitale occupent le champ d'une protection réglementée contre la cybercriminalité. Dans le cadre des Opérateurs d'Importance Vitale, la règlementation fait en sorte que ces derniers aient un régime contraignant en matière de protection contre le risque cyber. Cet élément de contrainte fait que les organismes qui y sont soumis doivent rigoureusement appliquer les conseils et les recommandations émis par l'Agence Nationale de la Sécurité des Systèmes d'Information. C'est notamment le cas, comme nous l'avons vu, des Grands Ports Maritimes. Au contraire, ceux qui ne sont pas soumis à cet élément de contrainte auront une marge de manœuvre quant aux démarches à adopter en matière de cybersécurité. Dans le cadre de l'industrie maritime, cette absence de contrainte peut très rapidement se transformer en défaillance dans l'exécution des mesures appropriées pour l'établissement d'une cybersécurité pérenne.

I Les causes de l'exécution défaillante

A - Causes psychologiques - Une mauvaise appréhension du risque cyber

1- Une appréhension insuffisante du risque

429. En premier lieu, la mauvaise appréhension du risque cyber tient au fait, selon Fabien Caparros, que ce dernier est analysé uniquement dans sa dimension technique. Par conséquent, les solutions apportées s'apparentent à des citadelles. Ces solutions sont insuffisantes. Elles deviennent bien trop rapidement contraignantes, si bien qu'elles sont rapidement inexécutées. Par ailleurs, ces approches ne prennent aucunement en compte les failles humaines, qui mettent dangereusement à découvert les systèmes en face des attaques. [57]

2- Un risque apparemment anodin

430. En second lieu, cette appréhension injuste tient au fait que le risque cyber est souvent minimisé. En effet, selon un auteur, si le crime cybernétique n'est pas vu comme un sujet majeur, cela tient au fait que plusieurs acteurs de l'industrie maritime considèrent que si les cyberattaques sont inévitables, l'organisation victime d'une attaque arrive rapidement à s'en relever[58].

3 - Un risque abstrait

[57] CAPARROS, F. *Managing the Cyber-Risk in the Maritime Industry* [en ligne]. Global Executive MBA/Strategic Business Project : Kedge Business School, 21 novembre 2017.

[58] UNDERHILL, S. Is the shipping industry embracing the digital age?. *Maritime Risk International*. 9 mars 2019.

431. En troisième lieu, certains acteurs minimisent la crédibilité des menaces. En effet, la plupart de ces dernières portent sur des systèmes d'information et non sur des navires. Cette circonstance contribue à ce que certains acteurs de l'industrie maritime ne se considèrent pas inquiétés par le risque cyber. Seules les menaces qui sont ressenties comme actives par l'entreprise font l'objet d'un traitement et d'un investissement. [5960]. Il résulte de cette indifférence que certains armateurs préfèrent des équipements ou logiciels peu onéreux, mais hautement faillibles et vulnérables à d'autres qui seraient mieux armés pour résister aux attaques ou aux bugs.

B) Causes économiques

1 - L'absence de retour sur investissement

432. Si l'on prend en compte les différents biais psychologiques susmentionnés, la suite logique est de constater que certains acteurs de l'industrie maritime peuvent considérer l'investissement dans la protection contre le risque cyber comme un coût sans nécessité. Par conséquent, le risque est bien souvent assumé, au vu de sa probabilité apparemment faible.

2 - La prépondérance de la réduction des dépenses

433. Il faut que les équipements permettant de diriger le navire et de le propulser soient totalement étanches. On sait aussi que les équipementiers s'efforcent de diminuer la consommation de carburant des moteurs, car l'armateur a. intérêt à consommer le moins de carburant possible. En effet, d'un point de vue concurrentiel, un navire consommant du carburant plus que la moyenne sera facturé plus cher à un client de l'armateur. Dès lors, ce dernier vendra beaucoup moins ses services en face de la concurrence. Donc on fait attention à la consommation de carburant, il y a une pression forte sur les

[59] Perfect storm of regulation, cost-savings and cyber security looms. *Maritime Risk International.* 2 août 2017.

[60] CAPARROS, F. *Managing the Cyber Risk In the Maritime Industry* [en ligne]. Strategic Business Project : Kedge Business School, 21 novembre 2017.

équipementiers et les fabricants de moteurs pour que le navire consomme le moins de carburant possible. A cette fin, on fait communiquer les moteurs en temps réel avec les fabricants pour indiquer le plus précisément possible la consommation pour telle charge et telle température. En retour le fabricant procède à des mises à jour des logiciels afin de proposer des options permettant une réduction de la consommation. Mais si les moteurs sont tous reliés à un même serveur, et fonctionnent selon des procédures mises à jour à l'extérieur, les vulnérabilités se multiplient.

434. Sur ce point, Louis Dreyfus Armement demande aux sociétés de classification que les équipements choisis soient classés hiérarchiquement selon leur degré d'ouverture informatique. Ainsi, l'armateur pourra choisir entre des équipements impossibles à mettre à jour à distance et des appareils connectés qui peuvent être monitorés à distance et réglés. Les premiers seront donc fermés et robustes, les seconds nécessiteront une équipe d'informaticiens se chargeant de la cybersécurité d'un tel équipement.

3 - Incidences de la construction navale sur la Cybersécurité du Navire

435. Chez Louis Dreyfus Armateurs, les navires de services sont construits sur le modèle d'un contrat à l'économie[61]. En effet, la coque est achetée à un chantier, puis l'armateur va faire installer à l'intérieur du navire les équipements qu'il choisira lui-même. Seront vraisemblablement choisis des équipements déjà connus, que les préposés de l'armateur ont l'habitude d'utiliser. Si tel n'est pas le cas, des formations sur ses équipements seront envisageables. Dans les navires de transports, cette procédure n'est pas aussi souple, selon Antoine Person. Le chantier sera susceptible d'imposer ses propres choix d'équipements. Les choix du chantier dépendront souvent de la taille du navire dont l'achat est considéré. Un armateur comme Louis Dreyfus pourra faire son choix d'équipements plus ou moins connectés selon la formation de ses équipages, les coûts qu'il est prêt à supporter, les risques qu'il est prêt à prendre. Dans la plupart des

[61] PERSON, A. [audio]. 2 juillet 2020.

navires de transport au contraire, un tel éventail n'est pas ouvert. Des équipements exigeant un usage précautionneux peuvent être confiés à des équipages peu formés.

II Les conséquences de l'exécution défaillante

A) La mise en place de technologies vulnérables

436. Les choix peu avisés évoqués ci-dessus font que certains éléments à haut risques sont présents au sein même des navires. L'on parle ici des aides à la navigation, tels que le Système d'Identification automatique, le Système de positionnement par satellite ainsi que celui de visualisation des cartes électroniques d'information. Ces systèmes souffrent de vulnérabilités de par leur conception.

437. La réglementation relative au Chapitre 5 sur la Convention Internationale pour la Sauvegarde de la vie humaine en mer en date du 1er juillet 2002 prévoit dans sa Règle 19 l'obligation d'équiper trois types de navires d'un Système d'Identification automatique. Sont soumis à cette obligation les navires de 300 tonneaux et plus effectuant des voyages internationaux, ceux de 500 tonneaux n'effectuant pas de voyages internationaux, ainsi que tout navire à passagers.

438. Il faut tout d'abord préciser que le Système d'Identification automatique AIS est basé sur un transpondeur. Il s'agit là d'un appareil qui reçoit et émet des ondes à hautes fréquences ayant 20 milles marins de portée effective. Ainsi, le système AIS permet une communication de navire à navire, mais aussi une communication navire-terre.

439. Les informations envoyées par l'AIS aux autres navires sont de trois ordres : dynamiques , statistiques et liées au trajet.

440. S’agissant des premières informations, il s’agit de la position du navire, de la date, de l’heure, de la vitesse et du cap, du Statut de navigation, du rayon de giration.

441. Les informations statistiques envoyées sont le numéro MMSI, le numéro IMO, le nom, le type, la longueur et la largeur du navire.

442. Enfin, peuvent être communiqués la nature de la cargaison, sa dangerosité, le Port de départ et le port de destination.

443. Si cet outil est fondamental pour l’aide à la navigation, il demeure hautement vulnérable face à des attaques extérieures.

444. En effet des produits sécurisant l’AIS existent. Il s’agit des AIS Secure Protocol. Toutefois, ces AIS sont utilisés en majeure partie par l’armée.

445. Le problème est à base que l’AIS procède à une diffusion en l’air, sans permettre de reconnaître qui est à sa source, ni si cette source est intègre. N’importe quel agent émettant un signal par ordinateur, peut incorporer ce qu’il souhaite dans la trame, et le message confectionné sera reçu par les navires. Avec un ordinateur et un émetteur, un adversaire peut affirmer passer par Gibraltar avec un pétrolier, alors qu’il se trouve à Paris. Mais un tanker sera identifié à Gibraltar ! Pour parer à ce risque, a été développé un AIS sécurisé permettant d’incorporer une signature.

446. Idem avec le GPS. Toutefois, les outils sont by design, de par leur conception, peu sécurisés.

447. On a développé un système de gestion de clés nécessaires pour ajouter la signature. Les clés d’identités devront être centralisées.

448. Cette technologie n’est pas seulement destinée à l’AIS. On peut se demander alors si l’AIS est encore très fragile.

449. Il est vrai cependant qu'on peut facilement brouiller l'AIS. Il suffit d'émettre une fréquence porteuse sur la fréquence de base. On peut donc duper le destinataire en envoyant de fausses positions. Ainsi, l'on peut créer une fausse piste.

450. Cette vulnérabilité du Système d'Identification Automatique le rend susceptible de détournement dans des buts hostiles. Ainsi, un AIS usurpé pourra permettre à un adversaire d'envoyer de fausses informations. Ces informations seront prises en compte par les navires environnants, les exposant à des abordages et à d'autres dommages connexes.

451. La question de la sécurité informatique n'a pas été prise en compte par la réglementation. En effet, la norme SOLAS a imposé des AIS pour les bateaux de plus de 300 tonneaux. Cette avancée était considérable pour la sécurité. Toutefois, la conception de l'AIS protège le navire mais l'AIS n'était pas sécurisé contre les attaques extérieures. La sécurisation n'a pas non plus été imposée par la réglementation.

452. L'absence de mesures visant à sécuriser un système non sécurisé par défaut pose une vraie question.

453. Car la sécurisation est tout à fait possible. Toutefois, un investissement bien plus important serait à envisager.

454. Deux possibilités pourraient être envisagées pour que ce manque soit comblé : la voie réglementaire ou les sollicitations du marché.

455. Aucune de ces approches n'est à ce jour suivie. En effet, cette faille n'est pas considérée suffisamment dangereuse dans l'industrie maritime pour donner lieu à une sécurisation généralisée des AIS.

456. Seuls, les militaires ont voulu disposer d'AIS sécurisés. L'AIS sécurisé a donc vite été développé pour le marché militaire. En effet, cette sécurisation répondait aux besoins des navires militaires face à des environnements hostiles.

457. Toutefois, dans le domaine civil, les menaces potentielles n'ont pas été concrétisées. Selon Fabien Caparros, personne n'aurait intérêt à attaquer l'AIS[62]. Dès lors, la sécurisation de l'AIS peut apparaître dans une certaine mesure comme un non-sujet.

458. En effet, ce n'est pas parce qu'il y a vulnérabilités qu'il y a risque. Un risque se concrétise en présence d'un acteur menaçant, susceptible de profiter des vulnérabilités.

459. Les différents Scénarios d'attaques sur l'AIS ne semblent pas non plus constituer un levier utile pour la piraterie en mer. Ainsi, on s'est demandé si les pirates somaliens utilisaient l'AIS pour trouver et attaquer leur cible. Devant la présence éventuelle de pirates, les navires vont couper l'AIS lorsqu'ils naviguent sur des zones à risques. L'utilisation de l'AIS à des fins criminelles est une éventualité peu probable.

460. Dès lors une amélioration technologique de la sécurisation pourra se révéler trop coûteuse, vu la faible probabilité du danger.

461. Du reste, utilisation de l'AIS par les Pirates somaliens n'a pas été avérée.

462. Ainsi, la vraisemblance des risques est faible. Cela ne signifie pas pour autant qu'ils ne se concrétiseront jamais.

463. La marine nationale a placé sous signe noir le risque que fait courir la situation actuelle de l'AIS. Il s'agit d'un risque pouvant avoir un fort impact. Toutefois, la

[62] CAPARROS, F. [audio]. 2 juillet 2020.

vraisemblance de ce risque est faible. En revanche, le risque que fait subir le GPS à l'industrie a été concrétisé.

464. Ce dernier, à l'instar de l'AIS, est facile à truquer pour leurrer les destinataires et facile à brouiller. En effet, le signal émis est extrêmement faible, de l'ordre 10^{28} Watts[63]. Par conséquent, si un signal parasite est déployé, le signal GPS peut devenir inexploitable très rapidement.

465. C'est précisément ce qu'ont exécuté des chercheurs de l'Université du Texas sur un SuperYacht où ils avaient été conviés[64]. En effet, à 30 milles marins de la côte, l'équipage ne peut se baser que sur des signaux GPS classiques, communiquant par orbite. Le signal étant faible, l'attaquant peut communiquer de fausses positions au GPS, qui pourra donc voir sa course déviée.

466. De surcroît, certains experts considèrent que ce mécanisme consistant à fausser la localisation des navires pourrait être utilisé par ces derniers pour leurrer les forces de l'ordre avec de fausses positions. Ces opérations auraient augmenté de 59 pour-cent[65].

467. Et de fait, en jouant sur l'intégrité du GPS, certains attaquant non identifiés ont mené en Mer Noire des attaques véritablement inquiétantes contre des navires[66].

---

[63] BAUDU, F. Les Cyber-Menaces contre les navires et les installations portuaires. *Gazette de la Chambre Arbitrale Maritime.* Printemps 2017, n°43, pp. 5 et 6.

[64] ZUMALT, E. Spoofing a Superyacht at Sea. *https://news.utexas.edu/* [en ligne]. 30 juillet 2013. Disponible à l'adresse : https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/

[65] DAVIES, N. Sophisticated Piracy : the new threat to the maritime sector. *Maritime Risk International.* 31 mars 2017, n°Avril 2017.

[66] Understanding GPS spoofing in shipping: How to stay protected. *https://safety4sea.com/* [en ligne]. 31 janvier 2020. Disponible à l'adresse : https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/?__cf_chl_jschl_tk__=620a4d65c27697bd92710bd2b5955d30764ca467-1598279096-0-AchZhN11FAAyn2Ks0WeES71jGoXNrGQgT0iA-KpXOXQO_QnwWV6ZJlGmhwhytpkjA_2M6YkXeLFaZN70dN4vaRf8ywFpc7xU8GSQkjJFc8aLTLPvY43nw9TMe51HEog7gWGJMyxLzkTrL4GZsATk54vLarXdMYgkR41AXA5mQZIwmWCGdGft_oF19Z78pIaYkDkuJHWAlkZXsqyes0nLNwlep58CKLLlfaW3L9QU8QkA0gkJWhhmxfRGDHoWYKtGyRRXdXwM6z68qM

B) L'impact du risque cyber sur les différents engagements

468. Cette absence de prise en compte du risque cyber peut également impacter les contrats principaux de l'industrie maritime. En effet, selon le cabinet d'avocat Holman Fenwick Willan, [67] la survenance d'un évènement cyber peut empêcher l'exécution d'un affrètement. Selon le document précité, la survenance d'un évènement cyber pourrait mettre en péril la navigabilité du navire et mettre en exécution la clause *off-hire*. Cette clause prévoit en effet qu'en cas de panne ou de dommages survenant sur le corps la machine ou les équipements ou si un évènement impactant le bon fonctionnement du navire survient, le paiement de l'affrètement pourra être stoppé. Le rapport préconise que l'évènement cyber soit clairement stipulé et défini dans cette clause.

469. Cette nécessité de prise en compte du risque cyber dans les différents contrats relève de sa clarté et de sa prévisibilité. En l'absence de directive claire, la cybersécurité doit faire l'objet d'une clause spécifique au vu des enjeux qu'elle revêt.

470. Comme il a pu être vu au cours de ce chapitre, l'exécution de mesures liées à une prise en compte réaliste du risque cyber est absolument fondamentale pour déterminer une protection pertinente contre la cybercriminalité. Il a pu également être évoqué le fait que l'exécution de ces mesures dépend également de leur caractère contraignant pour certains acteurs. Par conséquent, à moins que l'enjeu du risque cyber soit pleinement entendu, ces méthodes de gestion de risques peineront à être appliquées par l'ensemble des acteurs composant l'industrie maritime, a fortiori lorsque la mise en place d'investissements pour ce risque est considérée comme une perte.

MNQa01uhDFDFTTNbX6WVChFUDr78YITCLANYFJU7OLtonaOJYabV37ABM7ES_UHExoL4ag6a4l4ldnvWPz3vpvuz9P9kvk

[67] Cyber Pack. Holman Fenwick Willan, Juillet 2016.

471. Par ailleurs, d'autres solutions liées au choix des équipements du navire dans le cadre de la gestion des navires de services ont également pu être considérés. Toutefois, certains équipements modernisés permettent la réduction des coûts inhérents à l'exploitation du navire de marchandise. Il parait dès lors irréaliste de calquer les modalités de construction navale d'un navire de services sur ceux d'un navire de commerce.

472. Une première piste de solution tendant à mettre en place une cybersécurité au sein de l'industrie maritime pourrait peut-être consister en une gestion contractuelle du risque

CHAPITRE 2

- LA GESTION CONTRACTUELLE DU RISQUE : NEGATION ET RECONNAISSANCE

473. Le risque que fait courir la cybercriminalité est relativement récent. Nous avons vu qu'il avait largement été pris en compte tant au niveau mondial que par l'Union Européenne et par les autorités françaises.

474. Cependant au niveau des acteurs individuels, la prise de conscience est beaucoup plus inégale, un bon sens commun glissant trop facilement vers la négligence voire l'ignorance. Qu'en est-il donc au niveau intermédiaire, infra étatique, mais supra-individuel des relations contractuelles qui se nouent entre les armateurs et leurs partenaires le long de la chaîne d'approvisionnement ou au gré de l'assurance des navires ? là aussi, la situation est contrastée. Parfois ignoré le risque cyber est peu à peu reconnu, par la force des choses.

Section 1 - Le risque ignoré.

I Assurance Corps et Machines

475. Le risque cybernétique est presque entièrement exclu de l'assurance corps et machine, sous l'espèce de sa clause la plus utilisée, la clause 380, rédigée le 10 novembre 2003. Le 15 janvier 2019, Maître Sébastien Lootgieter en a donné la traduction libre suivante, dans le cadre du colloque sur le droit et la sécurité dans les transports qui se tenait à l'Université Paris-I Sorbonne :

476. *"1.1 Sous réserves des dispositions de l'article 1.2 ci-dessous, sont exclus les pertes et dommages, recours de tiers ou dépense résultant directement ou indirectement de l'utilisation ou l'exploitation, avec l'intention de causer des dommages, de tout ordinateur ou équipement informatique, programme ou logiciel informatique, virus informatique, code falsifié ou transmission de données, ou tout autre système électronique » ;*

1.2 : Si la présente clause fait l'objet d'un avenant à des polices couvrant les risques de guerre, guerre civile, révolution, émeute, insurrection, ou conflits en résultant, ou tout acte d'hostilité effectué par ou contre une puissance belligérante, acte de terrorisme ou toute action menée par des personnes agissant pour un motif politique, l'article 1.1 ne pourra pas exclure les pertes - dans la mesure où elles sont couvertes - résultant de l'utilisation de tout ordinateur, équipement informatique ou programme ou logiciel informatique, ou de tout autre dispositif électronique installé dans le système de lancement et ou de guidage, et/ou de mécanisme de mise à feu de tout arme ou missile"(Miribel, 18 février 2019) [68].

477. Sauf à racheter la clause, un assuré ne peut espérer aucune indemnisation concernant des dommages subis à cause d'attaques cybernétique, qui seraient seulement prises en compte dans le cas, peu fréquent où les conséquences informatiques d'un conflit violent, seraient couvertes par un avenant. Là encore, la formulation peu précise semble éloigner toute perspective d'indemnisation.

478. Cette exclusion de principe du risque cyber est liée à deux éléments, selon Fabien Caparros[69] (Caparros, 21 novembre 2017). Tout d'abord, les impacts potentiels d'une attaque cyber seraient dévastateurs pour une compagnie d'assurance. En effet, en cas de réalisation d'une attaque, il n'existerait aucune garantie quant à la limitation de cette dernière. Par ailleurs, rares sont les acteurs de l'industrie maritime communiquant sur les incidents subis. Dès lors, les compagnies d'assurance peinent à quantifier les montants qui devront être engagés face à une attaque de cet ordre. Par ailleurs, cette absence d'information rend encore plus laborieuse l'atténuation des attaques subies.

II Common Law

479. De surcroît, cette exclusion portera énormément préjudice à l'assuré si la police d'assurance est soumise à la loi anglaise. En effet, en vertu de la Common Law, un assureur est responsable d'une perte si et seulement si le péril assuré est la cause immédiate de ce dommage. Toutefois, une perte peut provenir de plusieurs causes différentes. En plus, conformément aux dispositions de l'International Underwriting

---

[68] MIRIBEL, S. Droit et Sécurité dans les transports aériens et maritimes. *Droit Maritime Français.* 18 février 2019, vol. 810.

[69] CAPARROS, F. *Managing the Cyber-Risk in the Maritime Industry* [en ligne]. Global Executive MBA/Strategic Business Project : Kedge Business School, 21 novembre 2017.

Association, lorsque l'on est en présence de deux causes immédiates pour un dommage, et que l'une des causes est exclue et l'autre prévue par la police, l'assureur pourra se baser sur la cause exclue pour l'ensemble du dommage. Ainsi, si une perte est notamment liée à une attaque cybernétique, les assureurs pourront refuser l'indemnisation, sauf à ce que la clause soit rachetée (Osler, 7 novembre 2018) [70]..

480. L'article précité affirme également que face au risque d'agrégation[71] que présente le risque cyber, certains acteurs de l'industrie de l'assurance maritime préconisent un élargissement encore plus poussé de la clause.

481. Du reste, l'on trouve également des polices corps ne mentionnant pas le dommage cyber. Ainsi, ce dernier n'est ni exclu ni compris dans la police d'assurance. Cette solution n'est pas non plus pérenne. En effet, d'un côté, les assureurs sont exposés à des risques dont ils ne pourraient pas effectivement assurer la couverture, et les bénéficiaires de la police d'assurance ne savent même pas s'ils sont couverts pour ce type de risques[72]. (Saul et Cohn, 12 janvier 2017).

Section II – Le risque reconnu

I Protection and indemnity clubs[73]

482. En sens inverse, il ressort des règles de l'International Group of P&I clubs que les responsabilités issues de l'usage du navire par l'armateur sont couvertes en cas de dommages issus d'une cyberattaque. Il existe toutefois une seule condition pour que la protection soit effective : que l'attaque ne relève pas du terrorisme, d'un acte hostile de la part ou contre un pouvoir belligérant ou de tout autre risque de guerre. Ainsi, la cybercriminalité pourrait potentiellement être couverte par les Protection and Indemnity

[70] OSLER, D. Needed : Innovation for Cyber-Risk Cover. *Maritime Risk International.* 7 novembre 2018, vol. Novembre 2018.

[71] Accumulation de demande en paiement en raison d'un seul évènement

[72] SAUL, J., COHN, C. Insurance gaps leave shipping exposed to growing cyber threats. *Reuters.* 12 janvier 2017.

[73] Les Protection and Indemnity Clubs s'apparentent a priori à une assurance responsabilité civile classique. L'assurance Corps et Machines assure l'armateur pour son navire. Le Protection and Indemnity Club assure quant à lui l'armateur pour l'usage de son navire.

Clubs[74] (O'Brien, 21 avril 2018). Il est à cet égard digne d'attention que la seule exclusion à cette protection soit justement le seul cas où il serait éventuellement possible d'indemniser un dommage dans un contrat corps et machine, c'est-à-dire si un avenant prévoyait explicitement le cas d'un conflit.

II Le partage de responsabilité d'un incident cyber.

483. Si elle diversement traitée par les compagnies d'assurances, en revanche, les armateurs regroupés dans le BIMCO ont émis des recommandations types claires sur la bonne manière de passer un contrat ; elles invitent à la prise en compte de la cybersécurité dans les dispositions liant les maillons de la chaîne d'approvisionnement. La « Cyber Security Clause » en date de 2019 comprend en substance les définitions et dispositions suivantes : « on entend par "Incident de Cybersécurité", la perte ou la destruction, l'altération, la divulgation, l'accès où le contrôle non-autorisés à un Environnement digital.

"Cyber Sécurité", les technologies, processus, procédures et contrôles conçus pour protéger les Environnements Digitaux d'Incidents de Cyber Sécurité.

"Environnement Digital", les systèmes technologiques d'information, les systèmes de technologies opérationnelles, les réseaux, les applications accessibles par Internet, les appareils, et les données contenues au sein de tels systèmes.

484. Chacune des parties devra :

(i) prendre les mesures et installer les systèmes adéquats de Cybersécurité, ainsi que déployer les efforts nécessaires pour maintenir sa Cybersécurité ;

(ii) mettre en place des plans et procédures appropriés afin de permettre de répondre à un incident de Cybersécurité de manière efficace et effective ;

(iii) évaluer régulièrement ses dispositifs de Cybersécurité, en vérifier l'application en pratique, maintenir la Cybersécurité et tenir à jour de la documentation attestant ce maintien.

---

[74] O'BRIEN, C. How Might Technology Affect the Marine Insurance Industry. *Maritime Risk International.* 21 avril 2018, vol. April 2018.

1. Toute partie devra déployer des efforts raisonnables pour garantir que toute partie tierce fournissant en son nom des services en lien avec ce contrat soit en conformité avec les stipulations des paragraphes (i)-(iii) de la présente clause
2. Si l'une des parties prend connaissance d'un Incident de Cybersécurité impactant ou susceptible d'impacter la Cybersécurité de l'une des parties, elle devra diligemment informer l'autre partie

485. Si l'incident de cybersécurité se déroule dans l'Environnement Digital de l'une des parties, cette partie devra :

-Prendre diligemment toutes les mesures qui sont raisonnablement nécessaires pour atténuer et/ou résoudre l'incident de Cybersécurité ;
-Dès que raisonnablement possible, mais pas dans un délai supérieur à 12 heures après la notification originale, fournir à l'autre partie les moyens de la contacter et toute information en sa possession susceptible d'aider l'autre partie à atténuer ou à prévenir tout effet de l'incident de Cybersécurité.

Chacune des parties devra partager avec l'autre partie toute information lui devenant par la suite disponible qui puisse aider l'autre partie à atténuer et/ou à prévenir tout effet de l'Incident de Cyber Sécurité.

La responsabilité issue d'une partie qui aura rompu une ou plusieurs fois la stipulation de cette clause ne devra jamais excéder un total de ----- (si laissé vide, de 100.000 dollars), à moins qu'il soit démontré que cette rupture est le seul résultat de sa négligence ou de sa faute volontaire. »

486.. Ces dispositions contractuelles mettent en exergue l'information réciproque et la nécessaire solidarité des différents chaînons de l'approvisionnement, solidarité intéressée s'il en est, chacun devant multiplier les « gestes barrière », pour ne pas risquer, mutatis mutandis, de s'infecter et, partant, d'infecter ses relations.

487.. Par ailleurs, dans le cadre de la négociation contractuelle, l'enjeu est pour les parties au contrat de déterminer si le risque cybernétique est inclus ou non dans la force majeure.

488. La force majeure se définit par son extériorité son imprévisibilité et son irrésistibilité. Elle permet donc d'écarter la responsabilité d'une partie au contrat si l'évènement générateur du dommage est inclus dans la force majeure. Cette négociation a souvent lieu selon Maître Henri Najjar entre le l'armateur et le l'affréteur notamment.

Ces clauses, d'un enjeu stratégique crucial, devront ensuite être validés parle P and I Clubs. (Najjar, 17 juillet 2020) [75]

489. Si une prise en compte progressive des problématiques liées à la cybersécurité a pu être mise en place, force est de constater que le manque d'exemples récurrents d'attaques cyber dans l'industrie maritime a pour conséquence principale que la réalité de ce risque est sous-évaluée par certains acteurs de l'industrie maritime. Par conséquent, les différents utilisateurs des systèmes d'information de l'industrie maritime peuvent ne pas être conscients de l'impact de leurs actions, mais surtout des menaces auxquels ils peuvent être exposés dans ce cadre.

490. C'est précisément ce manque de considération qu'il faut analyser afin de pouvoir quantifier son impact lors de la réalisation de différentes cyberattaques.

[75] NAJJAR, H. [audio]. 17 juillet 2020.

TITRE II L'INSUFFISANCE DE LA PRISE EN COMPTE DU FACTEUR HUMAIN POUR LA CONSOLIDATION D'UNE PROTECTION EFFECTIVE CONTRE LA CYBERCRIMINALITÉ

491. A la suite du piratage du Port d'Anvers en 2011, l'Agence Européenne chargée de la sécurité des réseaux et de l'information publie un rapport sur les Aspects de la Cyber sécurité dans le secteur maritime[76]. Le ton de ce rapport est intransigeant et dur. En effet, il est estimé que la conscience du risque cyber est basse, voire inexistante. Ce alors même que l'industrie maritime a de plus en plus recours aux technologies de l'information et de la communication. Ce manque de considération a pour conséquence que l'hygiène informatique et la prise de conscience du risque cyber par l'ensemble des personnes évoluant dans l'industrie maritime posent de vrais problème. L'hygiène informatique peut être définie comme l'ensemble des mesures qu'un utilisateur ou un informaticien devrait respecter afin de renforcer la sécurité d'un système d'information.

492. Par ailleurs, ce manque de prise de conscience a également pour conséquence d'augmenter le facteur humain, qui très souvent est la cause même de la réalisation d'une cyberattaque. Dans ce contexte, l'on peut définir le facteur humain comme l'ensemble des comportements et actes susceptibles de créer une insécurité informatique, ou pire, de permettre à une attaque de se réaliser.

493. Il faudra par conséquent analyser dans un premier chapitre la mise en place de l'hygiène informatique d'un système d'information (Chapitre 1), avant de se concentrer sur l'hygiène informatique des utilisateurs de ces systèmes (Chapitre 2).

[76] Analysis of the Cybersecurity Aspects in the Maritime Sector. Agence Européenne Chargée de la Sécurité des Réseaux et de l'Information, Novembre 2011.

Chapitre 1- La mise en place de l'hygiène informatique d'un système d'information

Section I L'importance de la mise en place d'une hygiène informatique[77]

494. La grande majorité des attaques cyber obéissent la plupart du temps à deux caractéristiques.

495. Elles ne ciblent pas en général une entreprise en particulier. Elles sont distribuées ou propagées après la première infection d'un ordinateur par un *exploit.* Il s'agit d'un code créé par des attaquants afin d'exploiter ou de viser la vulnérabilité d'un système. Ces exploits sont propagés dans un système informatique uniquement si des vulnérabilités dans ce dernier existent.

496. Ces vulnérabilités se situeront dans des logiciels déterminés. Dans ce cas de figure, les vulnérabilités résultent d'une imperfection, d'un bug ou d'une faiblesse, se trouvant dans un logiciel ou dans un système d'exploitation. Par exemple, constitue un bug le dépassement de tampon. A la suite de l'ouverture d'un dossier très volumineux, un autre logiciel ne répond plus ou chute. Cette faille peut parfaitement être utilisée par les attaquants. L'*exploit* sera créé et visera ce bug. Le logiciel de l'attaquant sera lancé, qui pourra alors avoir accès à un système critique.

497. En pratique, plusieurs personnes travaillant dans les technologies de l'information s'occupent exclusivement de la réparation de ces vulnérabilités. En résultat de cette recherche, les ordinateurs ont à leur disposition des propositions de mise à jour. Ces propositions consistent en des correctifs ou patches. Il s'agit de fragments de code permettant de corriger les vulnérabilités d'un programme.

[77] Notion englobant des règles élémentaires informatiques à appliquer pour la sécurisation des systèmes d'information

498. Ainsi, les vulnérabilités des systèmes informatiques peuvent être classés en trois catégories.

499. Les vulnérabilités peuvent d'abord être inconnues. Elles ne sont pas découvertes ou dévoilées. Puis, elles peuvent être connues mais non résolues. En pratique, ce type de vulnérabilités n'est pas dévoilé publiquement afin d'éviter que les attaquants s'en emparent. Si un *exploit* est disponible sur ce type de vulnérabilités, l'on parlera de failles *0-day*. Enfin, l'immense majorité des vulnérabilités sont connues et disposent d'une parade, grâce aux correctifs, ou aux nouvelles versions des logiciels.

500. Il faut bien garder à l'esprit que ce sont principalement ces failles qui sont utilisées par les attaquants qui essaient de les exploiter. Les probabilités que l'attaque menée se concrétise sont logiquement bien plus grandes dans un système non mis à jour que dans un système qui l'est.

501. Toutefois, comme il a été affirmé précédemment, les mises à jour ne sont pas souvent effectuées car les responsables trouvent superflu de réparer un élément qui fonctionne déjà.

502. Ce manque d'exécution a pour conséquence de ne pas pouvoir remarquer une attaque en train de se dérouler, tout simplement parce qu'aucun changement n'est a priori perceptible.

503. Un élément tout à fait problématique a été pointé du doigt par une étude menée par ESC Global Security[78] : dans le cadre de l'industrie maritime, 99 % des attaques auraient

[78] Maritime Cyber Security White Paper : Safeguarding data through increased awareness [en ligne]. ESC Global Security, Novembre 2015. Disponible à l'adresse : https://allaboutshipping.co.uk/wp-content/uploads/2015/11/ESCGS-Cyber-Security-WP-2015.pdf

pour origine les vulnérabilités précités. Or, 90 % de ces vulnérabilités disposent de correctifs.

504. Selon une autre étude[79], plusieurs acteurs de l'industrie du transport maritime sont réticents à mettre en place les correctifs sur leurs systèmes. Un premier argument consiste à affirmer qu'il est coûteux de télécharger l'ensemble des données. Puis d'autres peuvent arguer que les correctifs sont inutiles sur les ordinateurs non connectés à Internet. La responsabilité des mises à jour peut également être rejetée sur les équipages en charge de la gestion des marchandises.

505. Par ailleurs, la défaillance des mises à jour peut s'expliquer d'un point de vue psychologique. Il existe une tendance à croire qu'à la suite de la mise à jour, les logiciels ne seront pas opérationnels.

506. Enfin, dès lors que le système d'information est opérationnel, les utilisateurs ne souhaitent pas réparer un élément qui paraît fonctionner normalement.[80]

507. Comme il a été affirmé précédemment, les systèmes d'informations des entreprises se situant dans l'industrie maritime sont souvent connectés à des prestataires tiers, qu'il s'agisse des sièges sociaux des armateurs, des grands ports maritimes ou des navires. S'agissant des grands ports maritimes, leur statut juridique a pour conséquence d'être soumis à des recommandations obligatoire en termes de cybersécurité. Si les armateurs bénéficient d'un encadrement grâce à leur statut d'opérateurs de services essentiels, l'exécution des mesures peut souvent se révéler incomplète. C'est notamment le cas des

[79] HANNEMAN, W. Good IT hygiene is key to fighting cyber crime. *Maritime Risk International.* 13 décembre 2017, n°Décembre-Janvier 2018.

[80] HANNEMAN, W. Good IT hygiene is key to fighting cyber crime. *Maritime Risk International.* 13 décembre 2017, n°Décembre-Janvier 2018.

mises à jour, alors même qu'elles sont absolument essentielles pour une protection des systèmes vis-à-vis de nouvelles failles dans le système d'Information.

508. C'est précisément cette vulnérabilité qui a permis à l'attaque dirigée contre Maersk de prospérer.

509. Dans la filiale Ukrainienne de Maersk, l'installation du logiciel Medoc était rendue obligatoire afin de pouvoir communiquer avec le fisc ukrainien. Medoc a envoyé une mise à jour du logiciel à ses clients. Les attaquants étaient parvenus à mettre un virus du nom de Notpetya au sein de cette mise à jour. La mise à jour ayant été effectuée, chacun des ordinateurs a déployé la charge voulue par NotPetya le 27 juin 2017. Pour se propager à l'ensemble du système d'Information de Maersk, NotPetya a utilisé une faille du système Windows. Prénommé *Eternal Blue,* cet *exploit* avait été développé par la *National Security Agency* américaine. Il concernait le protocole *Server Message Block* de Windows. Cette faille avait été corrigée et publiée par Microsoft[81]. Dans le cas de Maersk, le correctif n'avait pas été appliqué[82].

510. Le virus Notpetya se présentait sous la forme d'un rançongiciel. Dès lors que la mise à jour avait été installée, un message apparaissait sur l'ordinateur attaqué. Le message indiquait que l'ordinateur avait subi l'attaque et que désormais, les fichiers y figurant n'étaient plus accessibles. En effet l'ordinateur avait subi un mécanisme de chiffrement d'un niveau militaire. Pour débloquer l'ordinateur, une rançon de 300 dollars à payer à travers le *DarkWeb* était demandé. En réalité, le virus avait une option *wiper,* permettant d'effacer des dossiers donc des données présentes sur l'ordinateur.

[81] Bulletin de Sécurité Microsoft MS17-010 - Critique. *docs.microsoft.com* [en ligne]. Disponible à l'adresse : https://docs.microsoft.com/fr-fr/security-updates/securitybulletins/2017/ms17-010

[82] CAPARROS, F. [audio]. 2 juillet 2020.

511. Cette attaque fut dévastatrice pour Maersk. Si la flotte était restée intacte, les terminaux et les systèmes d'information de Maersk ont dû être désactivés.

512. 4000 nouveaux serveurs, 25000 ordinateurs et 2500 applications ont dû être installés. L'évaluation du dommage financier subi s'élève à un montant évoluant entre 200 et 300 millions de dollars[83].

513. Cette nécessité des mises à jour, qui, comme nous l'avons démontré, peut se révéler dévastatrice si elles ne sont pas respectées, procède de l'hygiène informatique du système d'information. Cette hygiène doit également s'accompagner d'une prise de conscience du risque cyber par les différents utilisateurs d'un système d'information.

Section II - Les raisons de la négligence

514. Par ailleurs, l'absence d'efficacité des mises à jour tient au processus utilisé pour les mettre en place : si la mise à jour est faite à la main, il demeure probable qu'elle sera incomplète et inefficiente. Or, les mises à jour automatisées demandent des ressources financières et les Directeurs de Sécurité Informatique vont privilégier le fonctionnement effectif de leur système, plutôt que les mises à jour[84]. En effet, ces processus peuvent sembler une perte de temps au regard de l'efficacité nécessaire de l'industrie maritime.

515. Selon une autre étude[85], plusieurs acteurs de l'industrie du transport maritime sont réticents à mettre en place les correctifs sur leurs systèmes. Un premier argument consiste à affirmer qu'il est coûteux de télécharger l'ensemble des données. Puis d'autres peuvent arguer que les correctifs sont inutiles sur les ordinateurs non pas connectés à

[83] GARDNER, S. Cyber Risk in the Shipping Industry. *Maritime Risk International.* 5 septembre 2018, vol. Septembre 2018.

[84] CAPARROS, F. [audio]. 25 juillet 2020.

[85] HANNEMAN, W. Good IT hygiene is key to fighting cyber crime. *Maritime Risk International.* 13 décembre 2017, n°Décembre-Janvier 2018.

Internet. La responsabilité des mises à jour peut également être rejetée sur les équipages en charge de la gestion des marchandises.

516. Enfin, dès lors que le système d'information est opérationnel, les utilisateurs ne souhaitent pas réparer un élément qui paraît fonctionner normalement[86].

[86] HANNEMAN, W. Good IT hygiene is key to fighting cyber crime. *Maritime Risk International.* 13 décembre 2017, n°Décembre-Janvier 2018.

CHAPITRE 2- LA MISE EN PLACE D'UNE CONSCIENCE INFORMATIQUE CHEZ L'UTILISATEUR

Section I L'exploitation des failles humaines dans les cyberattaques

517. Plusieurs attaques dans l'industrie maritime mettent à profit les failles des utilisateurs ayant accès aux systèmes d'information des acteurs de l'industrie maritime.

518. Parmi elles, se trouve la fraude de paiement. La situation classique sera la suivante : l'armateur fait en sorte que l'un de ses navires fasse escale dans un port. Lors de son arrivée, l'armateur donnera le contact d'un agent maritime qui mettra à disposition du navire des provisions. L'agent maritime enverra alors une facture à l'armateur avec des informations bancaires pour le paiement.

519. L'attaquant aura déjà créé des fausses adresses mails et des comptes bancaires. L'adresse créée aura une seule lettre changée. Dès lors, si une attention particulière n'est pas portée au courriel, il sera compliqué de se rendre compte de la fraude.

520. De surcroît, l'attaquant aura déjà pénétré le système d'information de l'une des deux parties. Ainsi, après que le vrai courriel sera envoyé, les attaquants en enverront un second, affirmant que leur compte bancaire n'est pas opérationnel. Il sera alors demandé à l'armateur d'effectuer le virement sur un second compte.

521. Le courriel des attaquants ressemblera à l'identique au courriel légitime. Le paiement sera alors effectué sur le compte des attaquants.

522. L'agent pourra à juste titre se demander pourquoi le paiement n'est pas intervenu, et contactera l'armateur. Les deux parties se rendront alors compte qu'ils ont été victimes d'une fraude.

523. Dans ce cas de figure, les attaquants pourront ouvrir un compte bancaire sans pour autant dévoiler leur identité[87]. En effet, selon l'article précité, la présence de comptes bancaires à travers le monde fera que certains pays où sont situés ces comptes ne communiqueront par l'adresse des détenteurs de ces derniers. Par ailleurs, le *Darkweb* propose pléthore de moyens d'ouvrir un compte bancaire. A ce titre, le crime organisé peut employer des personnes pour ouvrir des comptes bancaires avec de fausses données d'identification. Il sera en effet laborieux pour une banque française ou anglaise de vérifier l'authenticité d'un passeport moldave ou tchétchène. Selon l'auteur de l'article précité, il est impératif que les utilisateurs soient formés à propos de ce genre de fraude. Ainsi des mesures de bases pourront consister en ne pas communiquer des informations personnelles ou bancaires par téléphone, mais surtout simplement poser des questions lorsque des informations contradictoires sont données à propos d'un paiement.

524. Par ailleurs, un attaquant pourra recourir à l'ingénierie sociale. Dans ce cas de figure, l'attaquant appellera un utilisateur en se faisant passer pour une personne de confiance. Elle tentera d'extirper des informations, notamment bancaires. Ou alors, se faisant passer pour le département informatique, l'attaquant pourra envoyer un fichier contenant un malware.

525. Une autre concrétisation s'est déroulée en 2011 dans le port d'Anvers. Un cartel de drogues néerlandais employait deux informaticiens pour pénétrer les systèmes d'information de deux terminaux à conteneurs et d'un opérateur portuaire. Pour ce faire, étaient utilisés des chevaux de Troie[88]. Le Cheval de Troie est un programme qui ne se réplique pas lui-même, mais ouvre l'accès des données à un pirate. Il est souvent greffé sur un logiciel piraté ou se fait passer pour un logiciel légitime. Il est en général caché dans un logiciel .exe, un fichier exécutable qui ne se mettra en route que si l'utilisateur clique sur ce fichier. L'attaque avait été prolongée par l'installation de *keyloggers*[89] sur les ordinateurs de la compagnie maritime. Ces objets permettaient de sauvegarder les données de

[87] THOMPSON, D. Cyber Security at Sea Critical. *Maritime Risk International.* 12 février 2018, vol. Février 2018.

[88] FLOCKHART, F., HADWIN, S., MANSIGANI, R. Time to take Stock of Cyber Risk. *Maritime Risk International.* 14 octobre 2017, vol. Octobre 2017.

[89] Objet permettant d'enregistrer l'utilisation d'un ordinateur

pwnie[90], également installés physiquement par les attaquants au sein des compagnies maritimes. *Les pwnies* étaient installés à l'intérieur de multiprises. Les pwnies étaient équipés d'un métasploit, qui permettaient de diffuser des données à travers les réseaux cellulaires. L'on pouvait accéder à ces données à partir de n'importe quel emplacement.

526. A partir de 2012, les employés de la compagnie se sont plaints de la lenteur des ordinateurs. La compagnie maritime opérant sur le port a fait appel à un investigateur privé. Ce dernier a fait appel a une société d'audit qui a découvert les *pwnies* et les *keyloggers*. Puis, la police a contacté les différents opérateurs du port. Il fut révélé que ces opérateurs avaient également subi la même attaque. Un des pwnies avait d'abord été retrouvé chez un opérateur, puis il avait été déplacé chez une autre compagnie chilienne. Une troisième compagnie dubaïote avait subi le même type d'attaques. A l'extérieur de cette compagnie, des caméras de surveillance montraient l'un des informaticiens avec une antenne attachée sur sa voiture. En outre plusieurs appels entre deux informaticiens montraient que ces derniers installaient directement les pwnies dans les compagnies portuaires.

527. Enfin, un chauffeur est venu récupérer un conteneur de moules le 21 novembre 2012. Le Code PIN donné n'était pas le bon. Il se trouve que le chauffeur avait présenté un faux bon de commande, le reliant directement au cartel de drogue. Se trouvait dans le conteneur 190 kilogrammes de cocaïne. Les informaticiens ont pu être arrêtés. Ceux qui les avaient engagés s'étaient échappés dans leur pays d'origine, en Turquie[91].

Section II La formation des utilisateurs

528. Dans le guide de l'Agence Nationale de la Sécurité des Systèmes d'Information[92], la première recommandation a trait à la sensibilisation des personnels vis-à-vis des questions de cybersécurité. 529. En effet, le rapport affirme que la prévention des cyberattaques et des incidents qui y sont liés

[90] petit ordinateurs dissimulés dans des objets électroniques, tels que des multiprises, permettant d'intercepter les données d'un système d'information

[91] RILEY, M., ROBERTSON, J. The Mob's IT Department. *www.bloomberg.com* [en ligne]. 7 juillet 2015. Disponible à l'adresse : https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/

[92] Guide des bonnes pratiques de Sécurité Informatique à bord des navires. Agence Nationale de la Sécurité des Systèmes d'Information, Octobre 2016.

peuvent être très souvent limités à l'aide de réflexes simples. Le guide préconise donc des séances d'information et une charte d'usage informatique. Les réflexes simples sont également présentés aux membres d'équipage.

530. Ces mesures sont communiquées notamment par L'Agence Nationale de la Sécurité des Systèmes d'Informations, qui a publié en 2018 un guide des bonnes pratiques de sécurité informatiques à bord des navires. Le guide est à la fois à destination des compagnies maritimes, mais aussi des équipages.

531. S'agissant des équipages, des mesures mettant en place une hygiène informatique sont préconisées. Ces mesures concernent aussi bien la sécurisation de l'usage privé des systèmes d'informations, que son usage public.

532. S'agissant de l'usage professionnel, la première recommandation a trait à l'établissement des mots de passe. Cet élément est fondamental. En effet, il s'agit du moyen principal d'authentification sur un équipement numérique. Il permet d'accéder à plusieurs données et d'effectuer plusieurs actions. Pour protéger ces éléments, un mot de passe fort est essentiel. Pour ce faire plusieurs règles sont à adopter. Tout d'abord, le code doit contenir au moins 8 caractères de signes différents. Ils ne doivent avoir aucun lien avec l'utilisateur et ne doivent pas pouvoir être trouvés dans le dictionnaire. Puis, un mot de passe utilisé à titre privé ne doit jamais être utilisé pour les systèmes d'information du navire. Ensuite, à chaque système sensible doit être attribué un mot de passe différent. Ces derniers ne doivent enfin pas figurer sur des post-it ou être enregistrés sur des logiciels internet généraux. Des logiciels spécialisés, tels que Keepass, approuvé par l'Agence Nationale de la Sécurité des Systèmes d'Information, devront être utilisés.

533. La seconde recommandation est liée à l'utilisation des messageries par l'équipage. Les courriels sont absolument fondamentaux pour les attaques informatiques. Les malwares où les virus sont souvent dans des mails frauduleux ou des pièces jointes piégées. Ainsi, le marin recevant un mail devra vérifier l'identité de l'émetteur en lui envoyant notamment un mail. Par ailleurs, les pièces

jointes issues de personnes inconnues ne devront pas être ouvertes. A ce titre, le téléchargement automatique des pièces jointes devra être désactivé.

534. Enfin, la séparation des usages personnels et professionnels semble fondamentale à l'établissement d'une cybersécurité pérenne. En effet, les équipements personnels sont susceptibles de porter atteinte à la sécurité des données du navire. En effet, la sécurisation d'un appareil personnel n'est aucunement du même niveau d'exigence que celle d'un système d'information. A ce titre, aucune information professionnelle ne devra être disponible à partir d'un smartphone, par exemple.

535. S'agissant ensuite de l'usage personnel, le guide appelle tout d'abord à la prudence des membres d'équipage dans l'usage privé qu'ils font d'Internet. En effet, les adversaires utilisent souvent des éléments issus de réseaux sociaux des équipages. Ainsi, des informations personnelles peuvent être collectées à l'insu des membres de l'équipages pour essayer notamment de deviner des mots de passe, ou alors d'adresser à ces derniers des courriers frauduleux personnalisés.

536. Puis, une autre recommandation a trait aux logiciels téléchargés sur les ordinateurs. Le téléchargement des logiciels sur les sites officiels est absolument fondamental. En effet, si cette mesure n'est pas suivie, le risque est l'exposition à des virus ou des Chevaux de Troie. Les Chevaux de Troie sont des logiciels malveillants permettant à celui qui l'emploie de prendre le contrôle ou de perturber le fonctionnement d'un ordinateur. L'attaquant envoie un mail à une personne et met une pièce jointe ou sera situé son Cheval de Troie. Si la personne télécharge ce logiciel, un mouchard sera installé sur son ordinateur. Le fichier d'installation se placera soit dans un programme fonctionnant normalement, comme un jeu ou le système d'exploitation windows[93] .Le facteur humain dans ce cas de figure est absolument fondamental

537. Au Grand Port Maritime de Marseille, une formation de 2H30 est dispensée à chaque agent[94]. Dans le cadre de cette formation, sont expliquées les règles de la charte utilisateur. En outre, un pan

[93] Le système d'exploitation est un ensemble de programmes permettant de diriger l'utilisation des ressources mises à disposition par un ordinateur

[94] FRANQUART, P. Les réponses du GPMM face aux Cyber Menaces/ Présentation au Café des Experts. 28 mai 2020.

entier de la formation consiste à appliquer les bonnes pratiques à mettre en oeuvre lors de l'utilisation des systèmes d'information. L'objectif principal semble quand même demeurer dans la prise en compte par l'utilisateur des conséquences de son comportement et de sa vigilance sur les systèmes d'information.

538. De surcroît, l'Autorité Qualifiée en Sécurité des Systèmes d'Information vérifie également le comportement des utilisateurs. A ce titre, sont effectuées des campagnes aléatoires où les responsables informatiques envoient aux utilisateurs des mails pouvant s'apparenter à des mails frauduleux. Dans ce cas de figure, l'attaquant est un agent de sécurité. Les utilisateurs qui sont tombés dans le piège en cliquant sur le courriel seront repérés. Une formation liée à la cybersécurité leur sera proposée. L'objectif est ici de sensibiliser les utilisateurs à une pratique qualifiée d'hameçonnage, où l'attaquant essaie de dérober les données personnelles d'un utilisateur par le biais d'un courriel pouvant susciter sa curiosité.

539. Enfin, les règles d'hygiène informatique auxquelles doivent se conformer les utilisateurs sont constamment rappelées à ces derniers. Parmi elles, l'on trouve notamment l'obligation de séparer les adresses emails professionnelles et les adresses mails personnelles. Par ailleurs, en cas de tentative d'attaque, un supérieur hiérarchique devra être contacté. En outre, les ordinateurs devront être éteints chaque soir sur les postes informatiques afin que les correctifs mentionnés plus hauts puissent être effectivement mis en place.

540. Ces évènements précités montrent la nécessité d'une formation accrue des utilisateurs en termes de cybersécurité.

541. Ces mesures sont communiquées notamment par L'Agence Nationale de la Sécurité des Systèmes d'Informations, qui a publié en 2018 un guide des bonnes pratiques de sécurité informatiques à bord des navires.

542. Le guide est à la fois à destination des compagnies maritimes, mais aussi des équipages.

TITRE II L'INSUFFISANCE DE LA PRISE EN COMPTE DU FACTEUR HUMAIN POUR LA CONSOLIDATION D'UNE PROTECTION EFFECTIVE CONTRE LA CYBERCRIMINALITÉ

543. L'on a pu voir au cours de ce mémoire que plusieurs éléments techniques juridiques et techniques constituent un socle commun suffisant pour que les différents acteurs de l'industrie maritime puissent mettre en place une protection contre la cybercriminalité.

544. Ce socle se compose de différentes normes, de systèmes matériels, et de méthodologies d'appréhension du risque cyber.

545. Que ce soit les normes, les systèmes matériels, tout ce qui est installé pour que les attaques cybernétiques ne prospèrent pas constitue d'excellentes initiatives.

546. Toutefois, la mise en exécution de ces socles peut s'avérer laborieuse en raison de la prise en compte faussée du risque cyber.

547. L'on pourrait dans ce cas de figure préconiser la mise en place de dispositifs législatifs contraignants qui concerneraient l'ensemble des acteurs de l'industrie maritime. Cette approche ne semble pas pérenne, car elle ne permet pas l'appréciation casuistique des risques cyber courus. Par ailleurs, cette stratégie pourrait mettre en péril l'attractivité d'un pavillon, et même des différents acteurs relevant d'un même pays.

548. Toutefois, l'on peut toujours imaginer que ces systèmes soient contournés. Dans ce cas de figure, la seule barrière contre la concrétisation d'une attaque, c'est l'utilisateur devant son écran.

549. Soit l'utilisateur est indifférent aux problématiques cybernétiques en raison d'une absence de formation, soit il est formé et prudent. Dans le premier cas l'attaque prospèrera. Dans la seconde, elle ne passera pas.

550. Par conséquent, même si les investissements liés à la cybersécurité représentent souvent plusieurs millions d'euros pour les armateurs et les Grands Ports Maritimes, la personne devant son clavier peut très souvent être celle qui arrête le virus.

551. C'est en cela que la sensibilisation de l'utilisateur des systèmes d'information est absolument primordiale.

552. A ce titre, la création de formations spécifiques liées à la cybersécurité maritime, à l'instar du très récent Mastère Spécialisé Cybersécurité des Systèmes Maritimes et Portuaires semble demeurer une solution pérenne.

553. Enfin, à titre particulier, le développement des formations liées à la cybersécurité au sein de l'ensemble des acteurs de l'industrie maritime semble demeurer un élément *sine qua non* d'une protection contre la cybercriminalité.

BIBLIOGRAPHIE

OUVRAGES GENERAUX

BONASSIES, P., SCAPEL, C. *Traité de Droit Maritime.* LGDJ. Lextenso.

MÉMOIRE OU THÈSE

CAPARROS, F. *Managing the Cyber-Risk in the Maritime Industry* [en ligne]. Global Executive MBA/Strategic Business Project : Kedge Business School, 21 novembre 2017.

OUHADJ, S. *La Mise en Application de l'ISM Code par les Compagnies* [en ligne]. Mémoire pour l'Obtention du D.E.S.S en Droit Maritime et des Transports : Aix-en-Provence : Aix-Marseille/Centre de Droit Maritime et des Transports, 1999

ARTICLES DE REVUES

ATMATSIDIS, K. Autonomous ships and The Cyber Security Challenge. *Maritime Risk International.* 2 avril 2019, n°Avril 2019.

BAUDU, F. Les Cyber-Menaces contre les navires et les installations portuaires. *Gazette de la Chambre Arbitrale Maritime.* Printemps 2017, n°43, pp. 5 et 6.

DAVIES, N. Sophisticated Piracy : the new threat to the maritime sector. *Maritime Risk International.* 31 mars 2017, n°Avril 2017.

DEVEREESE, G. Considering Cyber Threats in the Maritime Supply Chain. *Maritime Risk International.* 6 juin 2018, n°Juin 2018.

DE MAISON ROUGE, O. Transposition de la directive NIS- de la Cybersécurité à la Cyber-résilience. *Dalloz IP/IT.* pp. p.374.

DOUVILLE, T. Cybersécurité : transposition de la directive NIS, ses limites et ses conséquences. *La Semaine Juridique Edition Entreprise et Affaires.* 12 avril 2018, vol. 15-16, n°act. 284.

FLOCKHART, F., HADWIN, S., MANSIGANI, R. Time to take Stock of Cyber Risk. *Maritime Risk International.* 14 octobre 2017, vol. Octobre 2017.

GALATRY-ROLIN, E. Agence Nationale de la Sécurité des Systèmes d'Informations. *JurisClasseur Communication* [en ligne]. 28 février 2018, n°1000.

GARDNER, S. Cyber Risk in the Shipping Industry. *Maritime Risk International.* 5 septembre 2018, vol. Septembre 2018.

HANNEMAN, W. Good IT hygiene is key to fighting cyber crime. *Maritime Risk International.* 13 décembre 2017, n°Décembre-Janvier 2018.

LOOTGIETER, S. Cyber-Sécurité. *Gazette de la Chambre Arbitrale Maritime de Paris.* Printemps 2017, n°43, pp. 3-4.

LOOTGIETER, S. Les risques Cybernétiques dans le domaine des transports. *Droit Maritime Français.* 8 décembre 2015, n°775.

MIRIBEL, S. Droit et Sécurité dans les transports aériens et maritimes. *Droit Maritime Français.* 18 février 2019, vol. 810.

O'BRIEN, C. How Might Technology Affect the Marine Insurance Industry. *Maritime Risk International.* 21 avril 2018, vol. April 2018.

OSLER, D. Shipping is "decades behind" on cyber security, KPMG warns. *Lloyd's List.* 6 mai 2014.

OSLER, D. Needed : Innovation for Cyber-Risk Cover. *Maritime Risk International.* 7 novembre 2018, vol. Novembre 2018.

ROCHE, P. Safety Management, Due Diligence and Seaworthiness. *Maritime Risk International.* 21 avril 2018, vol. avril 2018.

SAUL, J., COHN, C. Insurance gaps leave shipping exposed to growing cyber threats. *Reuters.* 12 janvier 2017.

THOMPSON, D. Cyber Security at Sea Critical. *Maritime Risk International.* 12 février 2018, vol. Février 2018.

UNDERHILL, S. Is the shipping industry embracing the digital age?. *Maritime Risk International.* 9 mars 2019.

Perfect storm of regulation, cost-savings and cyber security looms. *Maritime Risk International.* 2 août 2017.

RAPPORTS

LE VEY, S. Evaluer et protéger le navire. Direction Générale des Infrastructures, Des Transports et de la Mer/Direction des Affaires Maritimes, Septembre 2016.

Dossier de Presse. Comité Interministériel de la Mer, 2018.

France, Comité Interministériel de la Mer, *Dossier de Presse.* 2019, 2019

Rapport Annuel [en ligne]. Armateurs de France, 2019.

Guide des bonnes pratiques de Sécurité Informatique à bord des navires. Agence Nationale de la Sécurité des Systèmes d'Information, Octobre 2016.

Port Cybersecurity : Good practices for the maritime sector [en ligne]. Agence Européenne Chargée de la sécurité des réseaux et de l'information, Novembre 2019.

ISO/IEC 27001 MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION. Organisation Internationale de standardisation, Novembre 2013.

Analysis of Cyber Security Aspects In the Maritime Sector. Agence Européenne Chargée de la Sécurité des Réseaux et de l'Information, 19 Décembre 2011.

The Guidelines on Cyber Security Onboard Ships [en ligne]. BIMCO, CLIA, ICS, INTERTANKO, INTERCARGO, IUMI, INTERMANAGER, OCIMF, World Shipping Council, 2018.

La défense en profondeur appliquée aux systèmes d'information. Direction centrale de la sécurité des Systèmes d'Information, 19 juillet 2004.

Livre Blanc sur la défense et la sécurité nationale. Direction générale des relations internationales et de la stratégie, 2013.

Maîtriser les risques de l'infogérance/Externalisation des Systèmes d'Informations". Agence Nationale de la Sécurité des Systèmes d'Information, Décembre 2010.

Cyber Pack. Holman Fenwick Willan, Juillet 2016.

Analysis of the Cybersecurity Aspects in the Maritime Sector. Agence Européenne Chargée de la Sécurité des Réseaux et de l'Information, Novembre 2011.

Maritime Cyber Security White Paper : Safeguarding data through increased awareness [en ligne]. ESC Global Security, Novembre 2015. Disponible à l'adresse : https://allaboutshipping.co.uk/wp-content/uploads/2015/11/ESCGS-Cyber-Security-WP-2015.pdf

TEXTES OFFICIELS

Organisation Maritime Internationale, *INTERIM GUIDELINES FOR MASS TRIALS* en ligne. 14 juin 2019.

Organisation Maritime Internationale, *n°MSC-FAL.1-Circ. 3 Guidelines on Maritime Cyber Risk Management* en ligne. 5 juillet 2017.

France, Agence Nationale de la Sécurité des Systèmes d'Informations, *Communiqué de Presse Externalisation, Cloud Computing : maîtriser les risques pour les systèmes d'information* en ligne. 3 décembre 2010.

PAGES INTERNET

HAND, M. Scale of cyber-security threat against shipping unknown: Bimco. *www.seatrade-maritime.com* [en ligne]. 25 octobre 2016. Disponible à l'adresse : https://www.seatrade-maritime.com/americas/scale-cyber-security-threat-against-shipping-unknown-bimco

RILEY, M., ROBERTSON, J. The Mob's IT Department. *www.bloomberg.com* [en ligne]. 7 juillet 2015. Disponible à l'adresse : https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/

EBIOS : la méthode de gestion des risques SSI Un outil simple et puissant. 2010. Disponible à l'adresse : https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-PlaquetteMetho-2010-04-081.pdf

www.larousse.fr [en ligne]. Disponible à l'adresse : https://www.larousse.fr/dictionnaires/francais/cybercriminalit%C3%A9/10910062

RISQUES Prévention des risques majeurs. [en ligne]. Disponible à l'adresse : https://www.gouvernement.fr/risques/risques-cyber

Glossaire. *www.ssi.gouv.fr* [en ligne]. Disponible à l'adresse : https://www.ssi.gouv.fr/entreprise/glossaire/c/

Lettre d'information Cyber Maritime n°3. *https://www.pole-mer-bretagne-atlantique.com/* [en ligne]. Avril 2020. Disponible à l'adresse : https://www.pole-mer-bretagne-atlantique.com/images/C2M2_Lettre_dinformation_CYBER_3_2020.pdf

Understanding GPS spoofing in shipping: How to stay protected. *https://safety4sea.com/* [en ligne]. 31 janvier 2020. Disponible à l'adresse : https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/?__cf_chl_jschl_tk__=620a4d65c27697bd92710bd2b5955d30764ca467-1598279096-0-AchZhN11FAAyn2Ks0WeES71jGoXNrGQgT0iA-KpXOXQO_QnwWV6ZJlGmhwhytpkjA_2M6YkXeLFaZN70dN4vaRf8ywFpc7xU8GSQkjJFc8aLTLPvY43nw9TMe51HEog7gWGJMyxLzkTrL4GZsATk54vLarXdMYgkR41AXA5mQZIwmWCGdGft_oF19Z78pIaYkDkuJHWAlkZXsqyes0nLNwlep58CKLLlfaW3L9QU8QkA0gkJWhhmxfRGDHoWYKtGyRRXdXwM6z68qMMNQa01uhDFDFTTNbX6WVChFUDr78YITCLANYFJU7OLtonaOJYabV37ABM7ES_UHExoL4ag6a4l4ldnvWPz3vpvuz9P9kvk

Bulletin de Sécurité Microsoft MS17-010 - Critique. *docs.microsoft.com* [en ligne]. Disponible à l'adresse : https://docs.microsoft.com/fr-fr/security-updates/securitybulletins/2017/ms17-010

ZUMALT, E. Spoofing a Superyacht at Sea. *https://news.utexas.edu/* [en ligne]. 30 juillet 2013. Disponible à l'adresse : https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/

AUTRES

FRANQUART, P. Les réponses du GPMM face aux Cyber Menaces/ Présentation au Café des Experts. 28 mai 2020.

annexe 1

Estimation rapide du besoin de sécurité d'un système d'information, Homologation de Sécurité, Agence Nationale de la Sécurité des Systèmes d'Information

Le tableau suivant permet d'évaluer les besoins de sécurité du système d'informa- tion (SI) à homologuer, en estimant la gravité des conséquences potentielles d'une défaillance du SI, la sensibilité des données, le potentiel des attaquants, le degré d'exposition aux menaces et l'importance des vulnérabilités intrinsèques du SI.

Si vous répondez « Je ne sais pas » à plus de deux questions, faites-vous aider par la maîtrise d'ouvrage, qui connaît les enjeux du système.

				Note
Question n° 1 : Votre système est-il important pour remplir vos missions ?				
1	***2***	***3***	***4***	
Non, le système est accessoire à l'accomplis- sement des missions	Oui, les missions seraient forte- ment perturbées par un dysfonc- tionnement du SI.	Oui, les missions dépendent totalement du SI	Je ne sais pas	
Question n° 2 : Si un sinistre atteint votre SI, causant un dysfonction- nement ou une perte de données, les conséquences en interne (pour vos ser- vices) seraient-elles graves ? *Exemple :* une panne électrique ne permet pas d'utiliser le système, le contenu d'une base de données a été supprimé, etc.				

				Note
1	*2*	*3*	*4*	
Non, les conséquences internes d'un sinistre seraient négligeables	Oui, les conséquences internes d'un sinistre seraient significatives	Oui, les conséquences internes d'un sinistre seraient graves, voire fatales	Je ne sais pas	
Question nº 3 : Si un sinistre touche la sécurité de votre système (il ne fonctionne plus ou pas bien, vol d'informations…), les conséquences pour l'extérieur (pour vos usagers, administrés…) seraient-elles graves ?				
1	*2*	*3*	*4*	
Non, les conséquences d'un sinistre pour l'extérieur seraient négligeables	Oui, les conséquences d'un sinistre pour l'extérieur seraient significatives	Oui, les conséquences d'un sinistre pour l'extérieur seraient graves, voire fatales	Je ne sais pas	
Gravité des conséquences potentielles (reportez ici la valeur maximale des réponses aux questions 1 à 3)				
Question nº 4 : Le fait que les données de votre système soient inacces- sibles est-il grave ? *Exemple :* vous ne pouvez pas accéder aux données en raison d'une panne matérielle.				
1	*2*	*3*	*4*	
Non, le fait qu'il ne soit pas accessible ne gêne quasiment pas l'activité	Oui, le fait qu'il ne soit pas accessible perturbera l'activité de manière significative	Oui, le fait qu'il ne soit pas accessible peut être fatal pour l'activité	Je ne sais pas	

				Note
Question nº 5 : Le fait que les données de votre système soient altérées est-il grave ? *Exemple :* un virus a modifié des valeurs dans une base de données, les remet- tant toutes à 0.				
1	*2*	*3*	*4*	
Non, le fait que les données soient altérées ne gêne quasiment pas l'activité	Oui, le fait que les données soient altérées perturbera l'activité de manière significative	Oui, le fait que les données soient altérées peut être fatal pour l'activité	Je ne sais pas	
Question nº 6 : Le fait que les données de votre système ne soient pas ou plus confidentielles est-il grave ? *Exemple :* la liste des bénéficiaires du service social est dévoilée.				
1	*2*	*3*	*4*	
Non, le défaut de confidentialité ne gêne quasiment pas l'activité	Oui, le défaut de confidentialité perturbera l'activité de manière significative	Oui, le défaut de confidentialité peut être fatal pour l'activité	Je ne sais pas	
Sensibilité des données du système (reportez ici la valeur maximale des réponses aux questions 4 à 6)				
Question nº 7 : Quel est le niveau de compétence maximal présumé de l'attaquant ou du groupe d'attaquants susceptibles de porter atteinte au système ?				

				Note
1	*2*	*3*	*4*	
Individu isolé de niveau de compétence élémentaire	Individu isolé de niveau de compétence avancé	Groupe d'indi- vidus organisés, de niveaux individuels de compétence faibles à moyens, ou individu isolé aux compétences expertes	Groupe d'individus experts, organisés, aux moyens quasi illimités	
Question nº 8 : Quelle est la précision des attaques potentielles envers le SI ?				
1	*2*	*3*	*4*	
Attaques « au hasard » sur le cyberespace	Attaques orientées vers le continent européen ou la France	Attaques ciblant un groupe de victimes présentant des caractéristiques communes	Attaques visant précisément le système	
Question nº 9 : Quel est le niveau de sophistication des attaques poten- tielles contre le SI ?				
1	*2*	*3*	*4*	
Outils d'attaque triviaux (logiciel de scan de ports, virus connus, etc.)	Outils élaborés génériques prêts à l'emploi (réseaux de botnet loués, faille connue, etc.)	Outils sophistiqués, adaptés pour le SI (zéro-day, etc.)	Boîte à outils très hautement sophistiquée.	

				Note
Question nº 10 : Quelle est la visibilité des attaques potentielles contre le SI ?				
1	*2*	*3*	*4*	
Attaque annoncée (revendications « d'hacktivistes », rançon, etc.)	Attaque constatée immédiatement par ses effets sur le SI	Attaque discrète, qui laisse des traces dans les journaux d'événements, mais ne perturbe pas le fonctionnement du SI	Attaque invisible, réalisée en laissant le minimum de traces	
Question nº 11 : Quelles sont la fréquence et la persistance des attaques potentielles contre le SI ?				
1	*2*	*3*	*4*	
Unique : l'attaque ne se produit sur la cible qu'une seule fois	Ponctuelle : l'attaque survient plusieurs fois sans régularité dans sa fréquence (elle peut être liée à l'actualité).	Récurrente : attaque par vagues successives importantes	Permanente.	
Base d'estimation des potentiels d'attaques cyber (reportez ici la valeur maximale des réponses aux questions 7 à 11)				
Question nº 12 : Quel est le niveau d'hétérogénéité du système ? *Exemple :* plusieurs logiciels, matériels ou réseaux différents pour un même système.				

				Note
1	*2*	*3*	*4*	
Le système est jugé comme homogène	Le système est jugé comme faiblement hétérogène	Le système est jugé comme fortement hétérogène	Je ne sais pas	
Question nº 13 : Quel est le degré d'ouverture/interconnexion du sys- tème ? *Exemple :* Internet, un autre système interne ou externe (celui d'un prestataire, d'une autre autorité administrative…)…				
1	*2*	*3*	*4*	
Le SI n'est pas ouvert	Le SI n'est ouvert qu'à des systèmes internes maîtrisés	Le système est ouvert à des systèmes internes non maîtrisés ou externes	Je ne sais pas	
Question nº 14 : Le contexte dans lequel se trouve le SI et ses composants (matériels, logiciels, réseaux) évolue-t-il régulièrement ?				
1	*2*	*3*	*4*	
Le SI et son contexte sont jugés stables	Le SI et son contexte changent souvent	Le SI et son contexte évoluent en permanence	Je ne sais pas	
Question nº 15 : Les composants du SI sont-ils mis régulièrement à jour ?				
1	*2*	*3*	*4*	
Les composants du SI sont tous tenus à jour en permanence	Une partie des composants du SI est régulièrement mise à jour	Les mises à jour sont effectuées de manière irrégulière	Je ne sais pas	

Exposition et vulnérabilités (reportez ici la valeur maximale des réponses aux questions 12 à 15)		
Additionner les valeurs maximales des réponses aux questions	**TOTAL**	

Avec ces résultats que l'on additionne, on estime ainsi le besoin de sécurité de son système :

Somme des quatre valeurs	Besoin de sécurité du système
De 4 à 6	1 - Faible
De 7 à 9	2 - Moyen
De 10 à 16	3 - Fort

annexe 2

Estimation rapide du niveau de maturité de l'organisme, Homologation de Sécurité, Agence Nationale de la Sécurité des Systèmes d'Information

Questions	Oui / Non
Les activités de sécurité sont-elles réalisées en utilisant des pratiques de base (bonnes pratiques de sécurité, référentiels de mesures…) ?	
Si la case précédente est à **Oui**, alors votre organisme a un **niveau de maturité élémentaire en sécurité**, *sinon, une démarche assistée est indispensable.*	
Les activités de sécurité sont-elles planifiées ?	
Les acteurs affectés à des activités de sécurité sont-ils formés (en interne ou par un organisme de formation) à la SSI (niveau de com- pétence en sécurité jugé suffisant) ?	

Certaines pratiques de sécurité sont-elles formalisées dans des documents spécifiques (procédures) ?	
Des mesures de sécurité sont-elles en place ?	

Le tableau suivant permet d'évaluer le niveau de maturité en sécurité de votre organisme.

Le niveau de maturité en sécurité ne correspond pas au niveau réel de sécurité, mais à la capacité de l'organisme à gérer les risques, pour chaque système d'informatio

Les autorités compétentes sont-elles informées des mesures effectuées ?	
Si toutes les cases précédentes sont à **Oui**, alors votre organisme a un **niveau de maturité moyen en sécurité.**	
Les processus de sécurité sont-ils définis, standardisés et formalisés (définir la stratégie, gérer les risques, gérer les règles, superviser…) ?	
Des acteurs spécifiques sont-ils affectés à la gestion des processus de sécurité et sont formés en conséquence ?	
L'organisme dans sa globalité soutient-il les processus de sécurité (les différents niveaux hiérarchiques…) ?	
Les processus de sécurité sont-ils coordonnés dans tout le périmètre choisi ?	
L'efficacité des mesures de sécurité en place est-elle mesurée ?	
Des audits sont-ils effectués pour vérifier la suffisance des mesures en place ? (Les mesures de sécurité effectuées sont-elles contrôlées [auditées] ?)	
Les processus de sécurité sont-ils améliorés en fonction des mesures de sécurité effectuées ?	
Si toutes les cases précédentes sont à **Oui**, alors votre organisme a un **niveau de maturité avancé en sécurité.**	

CHAPITRE 2- LA MISE EN PLACE D'UNE CONSCIENCE INFORMATIQUE CHEZ L'UTILISATEUR

TABLE DES MATIÈRES

RESUMÉ

In English : Efficient protection against cybercrime in the maritime industry implies the development of various processes.

Firstly, a legal basis is necessary to enable relevant institutions to proceed towards the implementation of cybersecurity.

Also, the semantics of cybersecurity shall be shared by all of the protagonists of the maritime industry, in order to develop cyber risk awareness. The different player's coordination is also necessary to build a chain of trust which is absolutely crucial because of the various interconnections within the different Information Systems of the Maritime Industry.

In France, the horizontal coordination of the maritime industry's protagonist is currently evolving since the creation of the *Conseil Cybersécurité du Monde Maritime* in 2019, as well as the building of a Coordination Center for Maritime Cybersecurity.

Furthermore, the creation of various guidelines by national and international entities helps in building a shared semantic.

In a legal perspective, both the Network and Information Security Directive of 6th July 2016 and the French *Loi de Programmation militaire* have established legal grounds for the implementation of Cybersecurity in the maritime Sectors. These legal ensembles

introduce the notion Operators of Essential Services as well as the notion of *Opérateurs d'Importance Vitale* in France. Furthermore, the International Maritime Organization has included through its Resolution MSC.428(98) the cyber risk management in the scope of the International Safety Management Code's Safety Management System.

Even though legal and technical elements are available to implement cybersecurity in the maritime sector, the actual limitation to effective protection has its roots in the execution of these elements. Even if the cyber risk is taken into consideration in various contracts, the complete awareness of cyber risk thanks to management processes proposed by the *Autorité Nationale de la sécurité des Systèmes d'Information* remains challenging. As many attacks remain unreported, and many biases against cyber risk's seriousness stay in force, the users are struggling to understand the actual scope of this risk's danger. This poor cyber awareness is highly complementary with poor cyber hygiene.

As seen through various attacks on the maritime sector, the attackers use extensively these weaknesses to perform their intrusions. Therefore, impeccable cyber hygiene in the maritime industry's IT specialists as well as thorough training courses seem to be crucial for the maritime industry's protection against cyberattacks

Keywords : Cyber Risk Management, Cyber Crime, Critical Infrastructures, Cyber Security

En Français :

Une protection efficace contre la cybercriminalité dans l'industrie maritime implique nécessairement le développement de divers processus.

Tout d'abord, une base légale est nécessaire pour que les organismes compétents déploient leur action.

De plus, la sémantique liée à la cybersécurité doit être communément partagée par l'ensemble des acteurs de l'industrie maritime. Le respect de cet impératif est nécessaire pour que s'opère une prise de conscience commune du risque cyber. Il faut aussi une coordination des différents acteurs pour que s'assemble dans ce domaine une chaîne de confiance, absolument primordiale en raison des nombreuses interconnexions entre les systèmes d'informations de l'industrie maritime.

565. En France, la coordination horizontale des différents acteurs est en cours de formation depuis la création du Conseil Cybersécurité du Monde Maritime en 2019 et l'ébauche du futur Centre National de Coordination de la Cybersécurité Maritime.

Par ailleurs, la création de guides directeurs aussi bien par des acteurs étatiques que par des acteurs internationaux contribue à la création d'une sémantique commune.

D'un point de vue légal, un droit commun de la cybersécurité existe désormais grâce à la Directive Network and Information Security du 6 juillet 2016 et à la Loi de Programmation Militaire du 18 décembre 2013. Ces deux socles juridiques consacrent la protection des Opérateurs de Services Essentiels et des Opérateurs d'Importance

Vitale. Par ailleurs, les nouvelles lignes directrices de l'Organisation Maritime Internationale intègrent le risque cyber dans le Système de Gestion de Sécurité.

Si un socle permettant la mise en place de ces trois strates existe, le réel obstacle pour la mise en place d'une protection effective réside dans l'exécution de ces recommandations. Alors qu'une contractualisation du risque cyber se met en place, la prise de conscience de ce risque au moyen de démarches préconisées par l'Autorité Nationale de la sécurité des Systèmes d'Information se révèle laborieuse. En effet, les réticences à signaler les incidents et d'autre biais psychologiques détournent les utilisateurs de reconnaître les dangers. Par conséquent, le risque cyber n'est pas perçu comme tel. Cette faible prise de conscience va de pair avec une hygiène informatique insuffisante. Au vu des attaques subies par différents acteurs de l'industrie maritime, c'est ce facteur humain qui constitue la brèche où s'engouffrent les attaques. C'est donc une hygiène informatique sans défaut chez les responsables des systèmes ainsi qu'un effort approfondi de formation qui permettront aux acteurs de l'industrie maritime de résister à ces nouvelles formes d'agression.

Mots Clés : Gestion de Risque, Cybercriminalité, Cybersécurité, Gestion de risque, infrastructures critiques