© Standret-Freepik

12

Cybersécurité maritime

Introduction

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) définit le cyberespace comme « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques »[1]. Le cyberespace est un espace numérique qui comporte trois dimensions : une dimension physique avec les ordinateurs et composants réseau, une dimension logique par l'architecture réseau et logicielle ainsi que les informations stockées, et une dimension sociale car il assure la mise en communication de différents acteurs.

Comme le soulignait le Livre blanc sur la défense et la sécurité nationale de 2013, « les systèmes d'information sont désormais une donnée constitutive de nos sociétés »[2]. Dès lors il est impératif que le cyberespace demeure un espace de confiance pour les acteurs publics, les entreprises et les particuliers. La cybersécurité, parfois nommée sécurité informatique ou sécurité des systèmes d'information, consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. Les systèmes de cybersécurité recouvrent tout le domaine numérique (bases de données systèmes de comptabilité ou RH…) et ont généralement un lien fort avec le monde physique, notamment par la mise en œuvre de dispositifs de contrôle ou de pilotage d'installations ou d'équipements. La cybersécurité permet de protéger les données numériques générées par un territoire et ses citoyens, mais aussi par les opérateurs économiques (entreprises, services publics…).

La première stratégie de cybersécurité de la France a été élaborée début 2010 et publiée début 2011[3], une seconde stratégie a vu le jour en 2015[4]. Plus récemment, la revue stratégique de cyberdéfense publiée en 2018, dresse un panorama de la cybermenace, formule des propositions d'amélioration de la cyberdéfense de la Nation et ouvre des perspectives visant à améliorer la cybersécurité de la société française. Cette revue marque le début d'une nouvelle stratégie de cyberdéfense fondée sur le durcissement de la protection des systèmes informatiques de l'État et des organismes d'importance vitale ainsi que le renforcement de la sécurité numérique pour les citoyens, les institutions et l'ensemble des acteurs qui participent au dynamisme économique, industriel, social et culturel du pays.

1 - ANSSI 2011, *rapport Défense et sécurité des systèmes d'information Stratégie de la France.* https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/ [Consulté le 05/04/2022].

2 - Site internet du SGDSN *Livre blanc sur la défense et la sécurité nationale.* Livre blanc sur la défense et la sécurité nationale (livreblancdefenseetsecurite.gouv.fr) [Consulté le 05/04/2022].

3 - ANSSI 2011, *Défense et sécurité des systèmes d'information, Stratégie de la France.* https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf [Consulté le 05/04/2022].

4 - ANSSI 2015, *La Stratégie nationale pour la sécurité du numérique.* La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr) [Consulté le 05/04/2022].

Une stratégie de cybersécurité s'organise généralement en trois temps. Le premier consiste à identifier les systèmes critiques et leur vulnérabilité et de développer des mesures de protection pour anticiper les attaques éventuelles. Le second correspond à la gestion de la menace ; la sécurité doit pouvoir détecter le plus rapidement possible l'attaque afin de la contenir tout en assurant la continuité des autres services. Enfin, le dernier temps est celui de la restauration des dommages causés par l'attaque. En parallèle, de la gestion de l'attaque cyber, il est important de savoir prendre en charge les effets induits par la crise, comme l'interruption de certains services et la perturbation logistique. La transformation numérique dans le domaine maritime et portuaire a engendré un grand besoin de cybersécurité maritime. Le recours croissant à l'usage des NTIC[5] dans le monde maritime, a permis aux filières de renforcer leur efficacité et de rester compétitives notamment dans le secteur du transport maritime, mais a renforcé leur expositions aux cybermenaces. Les cyberattaques ciblant les acteurs du monde maritime ne sont pas rares[6], et s'expliquent en grande partie par les importants volumes financiers générés par le secteur maritime. Le développement d'une cybersécurité maritime pour veiller à la sécurité et à la sûreté du monde maritime s'impose de plus en plus dans le secteur. Si les États commencent à prendre conscience de l'importance de la cybersécurité maritime, cette dernière n'en est qu'à ses débuts, notamment pour les acteurs de taille petite ou moyenne, auxquels aucune contrainte de type réglementaire ne s'applique. Le secteur militaire, plus acculturé à la sensibilité des données et des réseaux, a mis en œuvre plus tôt une véritable cybersécurité maritime.

5 - Les nouvelles technologies de l'information et de la communication.

6 - Le Journal de la Marine Marchande, *le retour des cyberattaques,* Adeline Descamps, 21 septembre 2021. https://www.journalmarinemarchande.eu/actualite/shipping/le-retour-des-cyberattaques [Consulté le 02/06/2022].

I. État des lieux de la cybersécurité maritime

1. Les transformations numériques du secteur maritime

Depuis plusieurs années, le transport maritime a initié des transformations numériques dans les infrastructures terrestres et dans les navires. La mise en œuvre de nombreux systèmes d'information (SI) et de réseaux informatiques a favorisé l'apparition de nouveaux risques ; les navires sont en permanence connectés à la terre *via* les systèmes informatiques, et peuvent subir des cyberattaques même lorsqu'ils naviguent en mer. Le Secrétariat général de la Défense et de la Sécurité nationale (SGDSN) a rappelé dans son instruction relative à la sécurité maritime[7] que la transformation numérique du secteur maritime engendrait inévitablement une forte exposition à des cyberattaques, autant sur des navires en mer ou à quai que sur des infrastructures portuaires. Ce sont les informations et les systèmes opérationnels à bord des navires, l'interconnectivité des systèmes, le développement de l'accès à internet, le manque de résilience sur les bâtiments (conçus avant l'existence même d'internet pour les plus anciens) et le manque de formation des équipages à la menace cyber qui rendent les filières maritimes vulnérables à ces attaques.

Les cyberattaques que subissent les navires visent principalement les systèmes informatiques (IT) et les systèmes opérationnels (OT). La vulnérabilité des navires face aux risques cyber a longtemps été ignorée mais tend à être de plus en plus considérée par les acteurs du monde maritime. Cette prise de conscience s'est accélérée ces dernières années avec la multiplication des cyberattaques envers de grandes compagnies maritimes mondiales comme Maersk en 2017, CMA CGM en septembre 2020 ou le port de Durban en 2021. Le cabinet de conseil en cybersécurité Naval Dome estime que les tentatives

7 - Secrétariat général de la Défense et de la Sécurité nationale, *instruction interministérielle relative à l'organisation et à la coordination de la sûreté maritime et portuaire,* 27 juin 2018. Instruction N° 230/SGDSN/PSE/PSN/NP. http://www.sgdsn.gouv.fr/uploads/2018/08/20180627-instruction-interministerielle-nxx-230-surete-maritime-portuaire.pdf.

de cyberattaques maritimes auraient augmenté de 400 % durant la crise sanitaire du Covid-19[8].

La mise en place d'une cybersécurité sur une flotte est complexe car elle doit être adaptée aux caractéristiques de chaque navire. De plus, les effets des cyberattaques sont souvent aggravés par le manque de formation des équipages des navires à ces menaces.

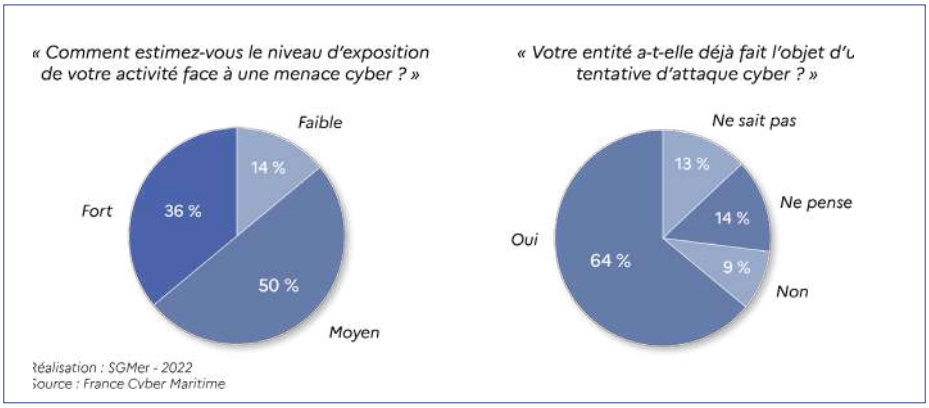


Figure n°1 : La perception de la menace cyber par les acteurs du maritime (enquête publiée en juillet 2020).

Ce n'est pas le fichier vectoriel, les corrections ne sont pas possibles. Merci de nous communiquer le fichier « ai. »

2. L'échelle des menaces cyber

D'après l'ANSSI, les cyberattaques ont généralement pour objectif l'espionnage, le sabotage, la déstabilisation et la cybercriminalité. Ces actions peuvent être commises pour des différents motifs et leur dangerosité se mesure par les moyens qui ont été investis pour l'opération (la compétence de technique de l'attaquant, la furtivité de l'attaque ou encore la probabilité que l'attaque compromette les SI de plusieurs navires). Ainsi, une attaque menée par un expert qui dispose de moyens quasiment illimités et qui est indétectable avant sa réalisation a une probabilité de succès beaucoup plus élevée qu'une attaque lancée par un utilisateur ayant peu investi dans l'opération, qui sera détecté pendant la phase de réalisation, voire avant.

Il existe donc un éventail de menaces ; la menace peut prendre la forme d'un logiciel malveillant dit maliciel dont la diffusion est incontrôlable, d'un attaquant solitaire disposant de moins de 100 € pour mener à bien son opération et dont le but principale est le jeu ou le profit, d'un employé malveillant qui possède un accès facile au navire et qui souhaite nuire à son employeur en mobilisant moins de 1 000 €, d'un groupe terroriste qui recherche à faire le plus de dégâts possibles afin que cela soit relayé par les médias et qui dispose entre 10 à 50 000 €, d'une entreprise criminelle

8 - Le journal de la Marine Marchande, *Les cyberattaques maritimes ont augmenté de 400%*, 5 juin 2020. https://www.journalmarinemarchande.eu/filinfo/rapport-les-cyberattaques-maritimes-ont-augmente-de-400 [Consulté le 02/06/2022].

possédant un budget se mesurant en millions d'euros et qui recherche la discrétion ou encore d'un État qui dispose de moyens presque illimités pour mener une attaque à bien avec discrétion.

L'ensemble des systèmes d'information à bord d'un navire[9] et des systèmes utilisés par les infrastructures portuaires ou les acteurs industriels peuvent être attaqués et sont susceptibles de causer préjudice à la navigation et, par conséquence, à la sécurité nautique. L'attaque d'un navire ou d'un port peut générer d'importantes conséquences pour le transport maritime mondial.

3. Les principales menaces cyber

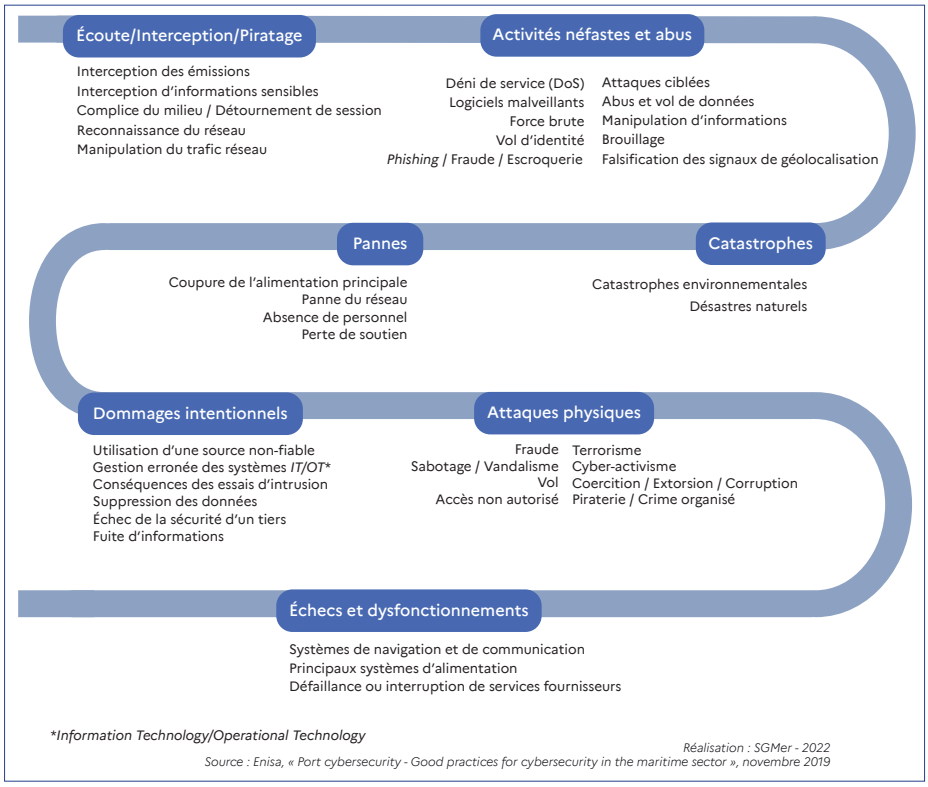


Figure n°2 : Panorama des principales menaces informatiques.

9 - Le système de visualisation de cartes marines (ECDIS), le système automatique d'identification (AIS), le système mondial de positionnement (GPS), les dispositifs de contrôle-commande, les postes de travail ou encore le système audio

A. Les menaces externes

Les attaques par rançongiciel

Un rançongiciel — ou *ransomware* en anglais — est un logiciel malveillant qui se transmet généralement par courriel *via* des pièces jointes ou *via* des liens de téléchargement sur Internet et qui provoque le chiffrement de toutes les données d'un ordinateur, les rendant illisibles par l'utilisateur. Si l'ordinateur ciblé est connecté au réseau, le maliciel va tenter de s'y propager et de compromettre d'autres ordinateurs ou systèmes d'informations. Le but de l'attaque par rançongiciel est de demander une rançon en échange de la clef de déchiffrement. Les rançongiciels entrainent la plupart du temps une perte de disponibilité des données ou une altération. Ce type d'attaque est fréquent car très rentable pour les attaquants.

Les attaques par hameçonnage ou phishing

L'hameçonnage est une technique d'attaque qui consiste à tromper des gens afin qu'ils transmettent des informations sensibles telles que des mots de passe, des coordonnées bancaires ou des identifiants de connexion à des services financiers, afin de lui dérober de l'argent. Les victimes peuvent recevoir des mails ou SMS qui les incitent à se rendre sur un site internet *via* un lien. Les utilisateurs qui cliquent sur ce lien sont redirigés vers des sites d'apparence légitime qui demandent généralement une authentification avec nom d'utilisateur et mot de passe. Si ces informations sont rentrées alors elles peuvent être utilisées par l'attaquant pour usurper l'identité, voler des comptes en banque ou encore vendre des informations personnelles. L'hameçonnage peut aussi être dit ciblé, c'est la technique du *spearphising* en anglais. L'attaquant usurpe l'identité d'une personne de confiance du destinataire souvent de collègues ou d'organismes importants afin d'obtenir des informations sensibles. Pour cela, il mène des recherches sur Internet et sur les réseaux sociaux afin de rendre le message plus crédible aux yeux du destinataire.

L'hameçonnage peut aussi être utilisé pour récupérer les informations (login et mot de passe) nécessaires pour accéder à un système d'information, qui est la véritable cible de l'attaquant.

B. Les attaques avec mise en place de dispositifs

Une cyberattaque n'est pas uniquement caractérisée par une infiltration dans des SI critiques d'un organisme, elle peut aussi désigner une intervention extérieure pour influencer des SI à l'aide de dispositifs techniques facilement concevables pour un informaticien non spécialiste en radiocommunication. Ce type d'attaque peut être utilisé par un État belliqueux désirant conduire des actions de déstabilisation et peut toucher les navires lorsqu'il s'agit notamment de brouillage ou de leurre du GPS sur des zones géographiques très fréquentées ou dans des zones de conflit. Ces actions peuvent avoir pour

conséquence des erreurs de positionnement des navires qui, en cas de grand trafic, sont particulièrement dangereuses car elles peuvent entraîner une proximité susceptible de provoquer des accidents. Elles peuvent aussi tromper la navigation d'un navire dans ses repères géographiques et le pousser vers de hauts fonds et donc provoquer un échouement.

C. Les menaces internes

Les attaques avec intervention du personnel employé

Si les cyberattaques font souvent intervenir des acteurs extérieurs, il existe aussi une menace interne. Tout personnel qui se rend sur son lieu de travail et qui est susceptible d'avoir accès à des ressources informatiques doit être considéré comme un chemin d'attaque potentiel[10]. La menace est dite interne puisqu'elle peut être liée aux salariés ou encore à des sous-traitants. Les cyberattaques de ce type peuvent avoir pour motif une vengeance personnelle menée par un salarié contre son employeur, une motivation financière ou être effectuée sous contrainte. Elles peuvent entraîner une modification des systèmes d'information volontaire et des dommages couteux. Toutefois, le cas le plus fréquent mettant en œuvre l'intervention d'un employé se fait à l'insu de celui-ci, en exploitant son manque de culture de cybersécurité (branchement de clef USB « personnelle » non blanchie, installations de logiciels non professionnels).

Les attaques dues à un branchement au réseau

Si un attaquant peut accéder à un réseau en compromettant des postes de travail, il peut aussi y avoir accès par des prises réseau se trouvant dans des zones accessibles au public. En branchant son ordinateur, la personne malveillante peut avoir accès à de nombreux systèmes. L'accès au réseau permet aussi d'atteindre d'autres cibles connectées à ce même réseau. Les navires peuvent aussi subir des cyberattaques à rebond c'est-à-dire que les attaquants commencent par infecter le SI du navire en se branchant au réseau pour ensuite atteindre une autre cible comme l'armateur qui possède un réseau connecté au SI du navire. L'attaque de sous-traitants pour pouvoir pénétrer le réseau de leur client est maintenant devenue courante.

10 - Guide ANSSI, *EBIOS Risk Manager,* septembre 2018. https://www.ssi.gouv.fr/uploads/2018/10/fiches-methodes-ebios_projet.pdf [Consulté le 02/06/2022].

II. Le cadre juridique de la cybersécurité maritime

1. L'échelle internationale

A. Les recommandations de l'Organisation Maritime Internationale (OMI)

L'OMI[11] est l'institution mondiale spécialisée dans la sécurité et sûreté des transports maritimes. À ce titre, elle édite des lignes directrices relative à la sécurité des navires. La circulaire MSC-FAL.1/Circ.3 contenant les directives sur la gestion des cyber-risques maritimes a été approuvée par le Comité de la simplification des formalités et le Comité de la sécurité maritime. Elle donne des recommandations de haut niveau sur la gestion des cyber-risques maritimes qui peuvent être incorporées dans des processus de gestion des risques existants. Cette circulaire a pour objectif de conseiller les armateurs et les opérateurs sur les opérations à mener pour sécuriser leurs cyber-systèmes dans l'entreprise et à bord des navires. Le Comité de la Sécurité Maritime (MSC) de l'OMI a adopté le 16 juin 2017 la résolution MSC.428(98) sur la Gestion des Cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité (SGS). Elle encourage les administrations à contrôler la cybersécurité maritime de leur système de gestion de la sécurité (SGS) au plus tard lors de la première vérification annuelle de l'attestation de conformité de la compagnie après le 1er janvier 2020. D'après la résolution, un SGS est approuvé si les cyber-risques sont gérés conformément aux objectifs et exigences du code international de gestion de sécurité (ISM).

11 - L'Organisation maritime internationale.

B. Les instruments obligatoires de l'OMI

Le Code international de gestion de sécurité (Code ISM)

Le Code ISM (International Safety Management) a été introduit en 1994 dans la Convention pour la sauvegarde de la vie humaine en mer (SOLAS) au chapitre IX « Gestion pour la sécurité de l'exploitation des navires ». Entré en vigueur en juillet 2002, ce code vise à renforcer la sécurité des transports maritimes internationaux et à mettre en œuvre un cadre international pour la sécurisation de la gestion et de l'exploitation des navires. La mise en place de ce système de sécurité relève de la responsabilité du propriétaire du navire ou de la personne exploitant le navire en tant qu'armateur ou affréteur à coque nue. Depuis 1998, le Code est obligatoire pour les navires-citernes, les navires à passagers et les vraquiers. Ce n'est que depuis 2002 qu'il s'étend aux navires couverts par la convention SOLAS. Les procédures obligatoires du code doivent être compilées dans un manuel de gestion de la sécurité dont un exemplaire doit être conservé à bord.

Le Code international de la sureté des navires et des installations portuaires (Code ISPS)

Par l'ajout d'un chapitre XI-2 « Mesures spéciales pour renforcer la sûreté maritime » de la Convention SOLAS[12] en décembre 2002, l'OMI a mis en place un instrument obligatoire pour les États Parties à la Convention : le Code ISPS. Entré en vigueur en juillet 2004, il comprend une partie A à caractère obligatoire avec des prescriptions sur la sécurité adressée aux acteurs du secteur maritime et une partie B non obligatoire qui porte sur les recommandations à prendre pour satisfaire ces prescriptions. Ce code vise à prévenir les actes illicites contre les navires et s'applique aux navires effectuant des voyages internationaux : les navires à passagers, les navires de charge d'une jauge brute supérieure à 500 et les unités mobiles de forage. Il s'étend aux navires à passagers effectuant des voyages nationaux à plus de 20 milles des côtes depuis le 1er juillet 2005 et à quelques catégories de navires opérant des liaisons maritimes nationales depuis le 1er juillet 2007. La certification des navires, qui comprend l'approbation du plan de sûreté des navires (SSP), la délivrance, le renouvellement et le visa des certificats de sûreté des navires assujettis au code ISPS, est organisée par le pavillon. Le SSP définit les mesures minimales, c'est-à-dire celles à mettre en œuvre en cas de risque de sûreté ainsi que les mesures spéciales pour les menaces imminentes. En France, la Direction des Affaires Maritimes (DAM)[13] est en charge du processus de certification. Par ailleurs, les infrastructures portuaires se voient délivrer une Déclaration de Conformité par l'État du port valable cinq ans. Pour cela, elles doivent élaborer une évaluation de la sûreté de l'installation portuaire qui doit porter sur l'accès à l'installation et un plan de sûreté de qui concerne l'intérieur

12 - La Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS) a été adoptée dans le cadre de l'OMI en 1974 et est rentrée en vigueur en 1980.

13 - La Direction des affaires maritimes (DAM) a fusionné au 1er mars 2022 avec la DPMA (la Direction des pêches maritimes et de l'aquaculture) afin de créer la Direction générale des affaires maritimes, de la pêche et de l'aquaculture (DGAMPA).

de ces mêmes installations afin d'identifier les mesures à prendre en cas d'attaque.

En l'état actuel, le code ISPS ne contient pas d'exigence spécifique concernant des mesures de cybersécurité, mais il serait le véhicule approprié pour en intégrer à l'avenir.

C. Les travaux complémentaires

UR E26 de l'IACS

L'IACS (*International Association of Classification Societies*)[14] a publié en avril 2022 une UR (*Unified Requirement*)[15], qui rassemble un certain nombre d'exigences de cybersécurité. Cette spéficiation unifiée s'appliquera à tous les navires devant être certifiés par une société de classification dont le contrat de construction sera signé à partir du 1er janvier 2024.

Groupe d'organisations internationales

Des lignes directrices ont été prises sur la cybersécurité et la cybersûreté à bord des navires afin d'assister les compagnies maritimes dans leur gestion des cyber-risques. Elles sont publiées par un groupe d'organisations internationales de transport maritime qui rassemble le BIMCO[16], l'Association internationale des lignes de croisière (CLIA), la Chambre internationale de la marine marchande (ICS), l'Association internationale des transporteurs de marchandises solides (INTERCARGO) et l'Association internationale des armateurs pétroliers indépendants (INTERTANKO). Elles se situent dans le prolongement de la résolution MSC.428(98)[17] et des lignes directrices de l'OMI ainsi que du cadre de NIST (voir *infra*). Ces lignes directrices ne sont pas des obligations mais des recommandations effectuées par le groupe qui considère que si la gestion des cyber-risques est propre à chaque compagnie, elle devrait être guidée par des réglementations nationales et internationales.

14 - L'IACS (l'Association internationale des sociétés de classification) est une organisation internationale non-gouvernementale qui est composée de douze sociétés de classification maritime. L'IACS établit des normes techniques pour la sécurité des navires et à la préservation du milieu marin.

15 - Les Unified requirement sont des résolutions adoptées par l'IACS qui permettent l'unification des règles de classification, des questions techniques ou de procédures. Les nouvelles règles édictées doivent être intégrées dans les référentiels techniques et les règlements respectifs des différentes sociétés de classification.

16 - BIMCO (*Baltic and International Maritime Council*) est l'une des plus grandes associations maritimes internationales d'armateurs.

17 - Résolution de l'OMI de juin 2016 sur la gestion des cyber-risques maritimes dans les systèmes de gestion de la sécurité. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

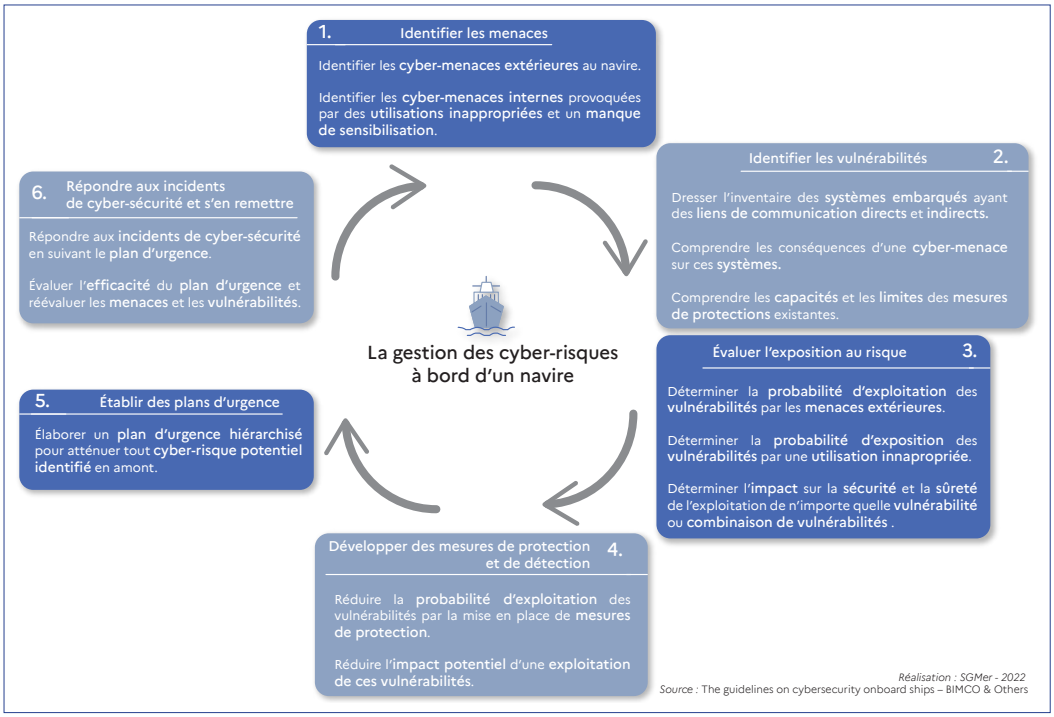


Figure n°3 : Approche de la gestion des cyber-risques telle que définie dans les orientations

Les cadres de la cybersécurité

La norme ISO/IEC 27001 :

Publiée en octobre 2005 puis révisée en 2013, la norme ISO/IEC 27001 est une norme internationale de l'Organisation Internationale de Normalisation[18] et de la Commission Electronique Internationale[19] qui fixe les exigences relatives aux systèmes de management de la sécurité des informations (SMSI)[20]. La certification ISO/IEC 27001 permet à une entreprise de montrer qu'elle possède des bonnes pratiques de sécurité.

Le cadre NIST :

Le cadre NIST est un cadre pour l'amélioration de la cybersécurité dans les infrastructures critiques issu d'un référentiel américain[21]. Cet outil de gestion des cyber-risques pour les organisations se structure autour de normes déjà existantes comme l'ISO 27001, le COBIT 5, l'ISA 624443 ou encore le CIS CSC. La mise en œuvre de ce cadre dépend de la maturité en termes de cybersécurité des entreprises. Le cadre NIST dispose de cinq niveaux de mise en œuvre : l'identification, la protection, la détection, la réponse et la récupération.

18 - Fondée en 1947, l'Organisation internationale de normalisation (ISO) élabore les normes internationales dans les domaines industriels et commerciaux.

19 - Fondée en 1906, la Commission électrotechnique internationale est la principale organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, l'électronique et les technologies apparentées.

20 - Un système SMSI est un ensemble de politiques visant la gestion de la sécurité de l'information et des données.

21 - Développé en 2013 par le *National Institute of Standards and Technology* le référentiel NIST avait pour objectif initial de définir un socle de mesures de sécurité pour protéger les infrastructures vitales et l'économie américaines. Il s'est imposé comme standard international incontournable de la cybersécurité.

2. L'échelle européenne

A. Le centre européen de compétence en matière de cybersécurité

Le centre européen de compétence en matière de cybersécurité (ECCC) a été créé en 2021[22]. Le Centre vise à renforcer les capacités et la compétitivité de l'Europe en matière de cybersécurité. Les principales missions du Centre sont :

- La mise en place et l'aide à la coordination du réseau des centres nationaux de coordination et la communauté de compétences en matière de cybersécurité ;
- La prise de décisions stratégiques en matière d'investissement et la mise en commun les ressources de l'Union européenne, de ses États membres et de l'industrie ;
- La mise en œuvre d'un soutien financier lié à la cybersécurité au titre du programme Horizon Europe[23] et des programmes pour une Europe numérique[24].

B. L'Agence Européenne de sécurité

Créée en 2004, l'Agence européenne de sécurité (ENISA) est en charge de la mise en place de la cyberpolitique de l'Union européenne. L'Agence travaille à la mise en de systèmes de certification en matière de cybersécurité visant à renforcer la fiabilité dans les nouvelles technologies de l'information et de la communication. Elle coopère aussi avec les États membres et les organes de l'Union européenne afin d'accroître la résilience de ses infrastructures et assurer la sécurité numérique des citoyens.

Dans son rapport de 2011[25], l'ENISA soulignait la fragilité de l'Europe sur la cybersécurité maritime et l'importance de développer une stratégie commune. Selon l'ENISA, le déploiement d'une stratégie européenne ambitieuse n'est possible que par l'harmonisation des politiques européennes et internationales et la prise en compte des enjeux spécifiques liés au secteur maritime.

22 - Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.

23 - Horizon Europe est le programme-cadre de l'Union européenne pour la recherche et l'innovation pour la période allant de 2021 à 2027. Le programme Horizon Europe prend la suite du programme Horizon 2020 qui s'est terminé à la fin de l'année 2020.

24 - Le programme Europe numérique 2021-2017 vise à soutenir et accélérer la transformation numérique de l'économie, de l'industrie et de la société européenne.

25 - ENISA, *Annual incident report 2011*. https://www.enisa.europa.eu/publications/annual-incident-reports-2011.

En novembre 2019, l'ENISA a publié un rapport sur les bonnes pratiques de cybersécurité pour les systèmes portuaires[26] en collaboration avec de nombreux ports européens dont HAROPA Ports, les ports de Valence, Trieste, Dublin, Anvers, Saint Nazaire, Tallin, Le Pirée, Brème, Rotterdam ou encore Amsterdam. Dans son rapport, elle expose les vulnérabilités des systèmes portuaires face aux cyberattaques et donne des recommandations aux autorités et opérateurs portuaires pour améliorer leur niveau de cybersécurité.

C. La directive Network and Information Security (NIS)

Adoptée par les institutions européennes le 6 juillet 2016, la directive *Network and Information Security* (NIS) est le premier élément de la législation européenne de cybersécurité et a pour objectif d'assurer une sécurité élevée commune pour les réseaux et les systèmes d'information de l'Union européenne.

Cette directive définit des mesures concernant la sécurité des réseaux et des systèmes d'information européens. Elle s'applique particulièrement aux opérateurs de services essentiels (OSE) et aux fournisseurs de services numériques (FSN).

Les FSN sont essentiellement les entreprises de cloud, de moteurs de recherche ainsi que les market place faisant plus de 10 millions de chiffre d'affaire ou employant au moins cinquante salariés.

Les OSE sont sélectionnés parmi la liste de services essentiels dressée par secteur d'activité, ils correspondent à des acteurs nécessaires au fonctionnement de l'activité économique et sociale du pays. La liste des OSE est établie par le Premier ministre sur les recommandations de l'ANSSI et des ministères du secteur concerné et doit être actualisée tous les deux ans par les États membres. En France, de nombreux OSE fluviaux et maritimes ont été identifiés[27] comme les sociétés de transport fluvial, maritime et côtier de passagers et de fret, les entreprises de maintenance des navires, les entreprises d'exploitation des infrastructures de transport par voie d'eau, les gestionnaires et exploitants de ports ou d'installations portuaires, les exploitants de services de trafic maritime.

Les principales orientations de la directive NIS sont :

- La notification des incidents sur les OSE ;
- La surveillance du réseau ;
- La mise en place d'un système de gestion des risques cyber ;
- La sensibilisation des collaborateurs ;
- La mise en place d'une procédure de gestion des incidents.

26 - Site internet de l'ENISA, *Rapport sur les bonnes pratiques de cybersécurité pour les systèmes portuaires*, novembre 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector [Consulté le 02/06/2022].

27 - Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036939971/.

La directive NIS a été transposée en droit national par la loi n°2016/1148 promulguée le 26 février 2018[28], son périmètre d'application a été défini par le décret d'application du 23 mai 2018[29].

Suite à une révision proposée par la Commission Européenne en décembre 2020, la directive NIS a connu un renforcement de ses obligations et a élargi le périmètre des acteurs concernés par des obligations réglementaires en matière de cybersécurité[30]. La NIS 2 s'applique à de nouveaux acteurs comme les fournisseurs de services de communications électroniques accessibles au public, les services numériques, le traitement des eaux usées et la gestion des déchets, la fabrication de produits critiques, les services postaux et de courrier et l'administration publique, aux niveaux central et régional. Elle couvre aussi plus largement le secteur des soins de santé. La directive NIS 2 renforce également les exigences en matière de cybersécurité imposées aux entreprises, traite de la sécurité des chaînes d'approvisionnement et des relations avec les fournisseurs et introduit le concept de responsabilisation des dirigeants en cas de non-respect des obligations en matière de cybersécurité. La directive contribuera à accroître le partage d'informations et la coopération en matière de gestion des cybercrises tant au niveau national qu'au niveau européen.

D. Le règlement général sur la protection des données (RGPD)

Le Règlement Général sur la Protection des Données (RGPD) a été publié le 4 mai 2016[31]. Le RGPD possède un important volet cybersécurité puisqu'il renforce les exigences en matière de sécurisation des données personnelles et vise à accompagner les administrations ainsi que les entreprises dans ce domaine. Afin d'assurer la conformité au règlement européen dans le temps, les organismes nomment un délégué à la protection des données (DPO) pour assurer un niveau de sécurité adaptées aux risques. Chaque pays a mis en place une autorité de contrôle local, en France, il s'agit de la Commission Nationale de l'Informatique et des Libertés.

Le RGPD crée des droits pour les personnes concernées et des obligations pour les responsables de traitement. Le RGPD impose la protection des données personnelles dès la conception avec des techniques d'anonymisation et le chiffrement des données. Ainsi, les entreprises doivent mettre en place

28 - Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772/.

29 - Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036939971/.

30 - Site internet de la Commission de l'Union Européenne, communiqué de presse du 13 mai 2022, *La Commission se félicite de l'accord politique relatif à de nouvelles règles en matière de cybersécurité des réseaux et des systèmes d'information* https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2985 [Consulté le 02/06/2022].

31 - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE). https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

des mesures techniques et organisationnelles pour sécuriser les données, tenir un registre des violations de données, effectuer une Analyse d'Impact sur la Protection des Données (AIPD), notifier la CNIL d'une violation de données dans un délai de 72h et informer les personnes concernées lorsqu'il s'agit d'un risque élevé. Le règlement concerne les entreprises européennes et les entreprises étrangères dès qu'elles traitent les données personnelles de citoyens européen. En cas de non-respect des règles du RGPD, les entreprises sont passibles d'amendes administratives pouvant atteindre 4 % du chiffre d'affaires mondial ou 20 millions d'euros.

3. L'échelle nationale

La France par son rang de puissance maritime et son expertise dans le cyber dispose d'une double légitimité dans le domaine de la cybersécurité maritime, notamment dans le secteur de la défense navale. La France souhaite améliorer la sensibilisation des filières du maritime à ces nouveaux dangers et mettre en œuvre une culture cyber qui permettrait de contrôler la sécurité dans l'ensemble du secteur.

A. La Loi de Programmation Militaire (LPM)

La Loi de Programmation Militaire (LPM) a pour objectif de préserver les intérêts vitaux de la France en terme de défense. La LPM de décembre 2013 a été le support législatif pour la transposition des grandes orientations de cybersécurité du livre blanc 2013 sur la Défense et la sécurité nationale[32]. Pour la première fois, la LPM oblige les Opérateurs d'Importance Vitale (OIV)[33] à sécuriser leurs systèmes d'information d'importance vitale (SIIV). Depuis mi-2016, l'État publie des arrêtés sectoriels pour préciser la démarche de sécurisation que les OIV doivent suivre ; le décret concernant le transport maritime et fluvial a été publié en août 2016[34]. En cas de non-respect à ces obligations, le dirigeant de l'OIV est passible d'une amende de 150 000 € pour une personne physique et 750 000 € pour une personne morale.

32 - *Livre blanc, Défense et sécurité nationale,* 2013. http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

33 - Les Opérateurs d'Importance Vitale (OIV) sont les opérateurs qui exploitent les installations indispensables à la vie du pays. Ils sont désignés par le ministère coordonnateur selon une procédure interministérielle. On compte 12 Secteurs d'Activité d'Importance Vitale (SAIV) répartis en 4 groupes : l'activité humaine (alimentation, gestion de l'eau, santé), l'activité régalienne (activités militaires, judiciaires, civiles de l'État), l'activité économique (énergie, finances, transports) et l'activité technologique (communications, audiovisuel, industrie, espace et recherche). Un Plan de sécurité d'Opérateur d'Importance Vitale (PSO) adapté doit être conçu et mis en œuvre par chacun des 249 OIV français.

34 - Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transports maritime et fluvial » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033063081.

B. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au Secrétariat général de la Défense et de la Sécurité nationale[35], est en charge de la sécurité du numérique français. L'ANSSI a été créée en 2011 afin de répondre aux besoins identifiés par le Livre Blanc de la Défense et de la sécurité nationale publié par le Ministère des armées en 2008[36]. La mission première de l'ANSSI était le déploiement d'une stratégie nationale pour la sécurité des systèmes d'information face à la menace cyber.

Les lois de programmations militaires de 2013 et 2018 ont élargi les missions de l'ANSSI. L'Agence est désormais en charge ainsi en charge de la défense et de la sécurité des systèmes d'information de l'État. Elle dispose d'un pouvoir réglementaire lui permettant de fixer les règles devant être mises en œuvre par les opérateurs d'importance vitale en matière de protection de leurs systèmes d'information d'importance vitale, d'un pouvoir de certification et qualification des produits et services, et enfin du pouvoir, en cas de crise majeure, d'imposer des mesures à ces opérateurs.

Face la hausse des cyberattaques dans le secteur maritime, l'ANSSI a publié en coopération avec la Direction des affaires maritimes (DAM)[37] et une douzaine de compagnies maritimes françaises, un « guide des bonnes pratiques de sécurité informatique à bord des navires »[38] en mars 2015 afin de sensibiliser les équipages et les compagnies à ces nouvelles menaces. Deux nouveaux guides ont été publiés par la DAM et la DGITM[39], le « guide Cyber sécurité évaluer et protéger le navire »[40], publié en 2016 qui indique les grands axes à suivre pour mettre en place une gestion de la sécurité des systèmes d'informations et de communications à bord du navire, et le « guide Cyber sécurité renforcer la protection des systèmes industriels du navire »[41], publié en 2017, qui vise à sensibiliser les compagnies maritimes aux cybers risques spécifiques de l'internet industriel à bord du navire afin d'y adapter des règles d'usage préconisées en fonction du risque.

35 - Le SGDSN est un organisme interministériel placé sous l'autorité du Premier ministre français.

36 - Le livre blanc publié par le Ministère des armées en 2008 est le premier document stratégique qui identifie le cyberespace comme étant un espace particulièrement stratégique pour la Défense française.

37 - La Direction des affaires maritimes (DAM) a fusionné au 1er mars 2022 avec la DPMA (la Direction des pêches maritimes et de l'aquaculture) afin de créer la Direction générale des affaires maritimes, de la pêche et de l'aquaculture (DGAMPA).

38 - Site internet de l'ANSSi, *Guide des bonnes pratiques de sécurité informatique à bord des navires,* mars 2015. https://www.ssi.gouv.fr/uploads/2016/10/bonnes_pratiques_securite_informatique_maritime_anssi.pdf [Consulté le 02/06/2022].

39 - Direction générale des infrastructures, des transports et des mobilités.

40 - Guide DAM/DGITM, *Cyber sécurité évaluer et protéger le navire,* septembre 2016. Cyber sécurité Evaluer et protéger le navire (ecologie.gouv.fr). [Consulté le 02/06/2022].

41 - Guide DAM/ DGITM, *Cyber sécurité renforcer la protection des systèmes industriels du navire,* janvier 2017. Le risque industriel à bord du navire (ecologie.gouv.fr). [Consulté le 02/06/2022].

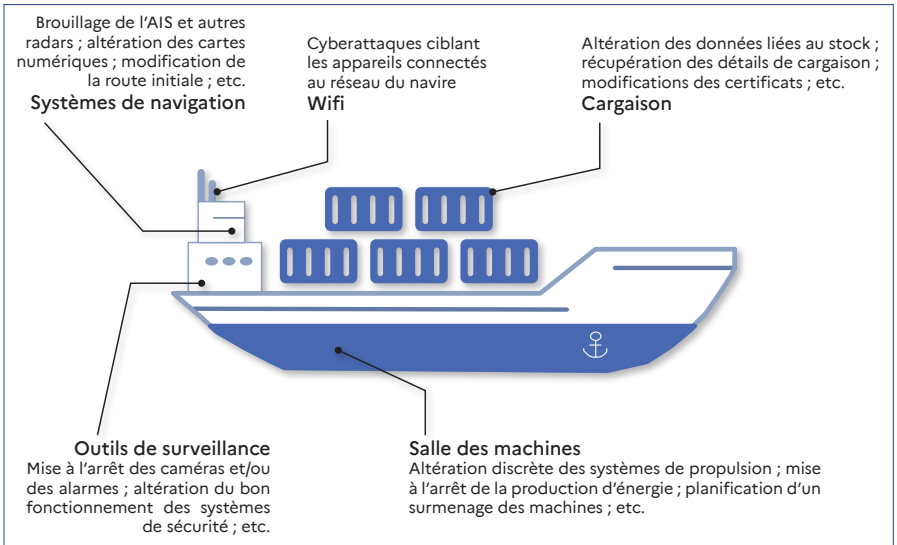
III. Les enjeux économiques

1. La cybersécurité du navire

A. Les vulnérabilités du navire

L'augmentation du nombre de systèmes embarqués et l'installation de nouvelles technologies interconnectées avec des réseaux internes industriels dans les navires amplifie le risque de cyberattaques.

Les navires sont d'autant plus vulnérables que les équipages ne sont pas permanents et que beaucoup d'intervenants sont susceptibles d'avoir un accès physique au SI du navire, ou à un point de connexion. Un SI regroupe l'ensemble des ressources nécessaires à la collecte, au stockage et au traitement de l'information. À bord d'un navire, plusieurs équipements sont sensibles à des cyberattaques.



Réalisation : SGMer - 2022
Sources : Aude-Marie Thomas, « Les six failles cyber du transport maritime », L'Argus de l'assurance, 26 février 2016 ; Rapport « Cyber sécurité » du Ministère de l'environnement, de l'énergie et de la mer - Septembre 2016

Figure n°4 : Les principaux éléments de la vulnérabilité d'un navire.

Les navires sont composés de différents systèmes :

Les systèmes élémentaires qui comprennent des capteurs et des censeurs générant différentes données ou service.

Les systèmes complexes pouvant comprendre plusieurs systèmes élémentaires. Les systèmes complexes fonctionnent à l'aide d'algorithmes, ils aident à la décision liée à la conduite des services métiers.

Les systèmes de « communication » permettant de relier le navire en mer à la terre.

Les systèmes « voyages » comprenant les modes de propulsion et la production d'énergie sont particulièrement vulnérables. Ainsi à bord des navires, les systèmes les plus vulnérables sont ceux qui sont nécessaires à la bonne conduite d'un navire dont les principaux sont : l'ECDIS[42], l'AIS[43] et le système satellite de navigation mondiale (GNSS).

B. L'impact des cyberattaques sur les navires

Les navires peuvent subir différentes cyberattaques :

- Les navires peuvent être confrontés à des attaques par rançongiciels qui se révèlent très dangereuses lorsqu'elles ciblent les SI nécessaires à la bonne conduite d'un navire. Ce type de logiciel malveillant est généralement introduit à bord lors d'intervention de sous-traitants (maintenance), par le biais d'ordinateurs personnels de l'équipage ou par le téléchargement de pièces jointes et devient hors de contrôle lorsqu'il se propage dans un réseau dit « à plat » c'est-à-dire non cloisonné.
- Les navires peuvent être la cible d'attaques par hameçonnage – qui visent généralement les compagnies maritimes –. Les équipages peuvent être victimes de ce genre d'attaque *via* leur boîte mail. Une fois activé, le maliciel peut se propager sur le réseau du navire et compromettre ses SI s'il n'y a pas de cloisonnement ou s'il est mal respecté. Les navires de la flotte peuvent alors faire face à des pannes inexpliquées d'équipements, la compagnie maritime est contrainte d'immobiliser sa flotte, entraînant une détérioration de son image ainsi que la perte de chiffre d'affaire.
- Les navires peuvent aussi être confrontés à des techniques de brouillage et à des leurres de GPS sur des zones géographiques très fréquentées. Ces actions peuvent provoquer des erreurs de positionnement des navires qui en cas de grand trafic sont particulièrement dangereuses car elles peuvent entraîner une proximité susceptible de provoquer des accidents. Elles peuvent aussi tromper la navigation d'un navire dans ses repères géographiques et le faire s'échouer.
- Les navires sont fortement exposés à des cyberattaques liées au personnel disposant d'un accès physique ou logique aux SI d'un navire.
- Enfin, les cyberattaques peuvent être dues à des branchements au réseau. Ce type de menace est particulièrement élevé avec les navires à passagers qui disposent de nombreuses prises accessibles. Un branchement au réseau permettrait alors à une personne malintentionnée d'avoir accès au système de gestion des télévisions, le système audio et le système d'alerte du navire. Si l'accès au réseau n'est pas contrôlé, l'intrus pourrait par exemple diffuser des messages à contenu violent pour susciter des mouvements de foule et de panique. La réputation de la compagnie maritime serait également alors impactée.

42 - Le système électronique d'affichage graphique et d'information (*Electronic Chart Display and Information System*).

43 - Le système d'outil et une aide à la navigation (*Automatic Identification System*). Il permet de transmettre aux navires (équipés d'un récepteurs), les informations relatives aux navires émetteurs (position, cap, vitesse, route...) dans un certain rayon. Il permet surtout aux navires qui émettent d'être visibles malgré des conditions difficiles et d'éviter les collisions.

Plusieurs mesures doivent être prises afin de protéger les navires et de renforcer leurs capacités de résistance face à de potentielles cyberattaques. Les équipages doivent être formés à la cybersécurité et sensibilisés aux cyberattaques, notamment celles liés à l'utilisation de la messagerie électronique, afin qu'ils soient plus prudents dans l'utilisation du matériel informatique. Des systèmes de surveillance du réseau doivent être installés pour repérer toute activité anormale. La capacité de cloisonnement du réseau est nécessaire pour éviter, en cas d'intrusion, la propagation du rançongiciel dans le réseau et la compromission d'autres systèmes. Ce cloisonnement consiste en une segmentation de l'architecture réseau pour limiter les conséquences d'une intrusion. Le rançongiciel peut aussi s'introduire dans le SI en exploitant une liaison Wi-Fi vulnérable lorsque le navire est relié au quai et causer sa paralysie. C'est pourquoi les points d'accès Wi-Fi doivent être sécurisés par chiffrement et une authentification par mot de passe doit être évitée. En prévention, une sécurité physique doit être mise en place dans les zones sensibles du navire comme la salle de commande ou machine afin de contrôler l'identité de chaque personne étant autorisée à y avoir accès avec par exemple un système d'accès par badge. Les SI critiques doivent aussi être surveillés afin d'éviter des modifications malveillantes. Les prises réseaux accessibles au grand public doivent être désactivées ou fortement contrôlées.

C. Étude de cas : les compagnies maritimes face aux menaces cyber

Depuis quelques années, l'accélération de la digitalisation des navires et des ports a renforcé l'exposition des compagnies maritimes internationales à la menace cyber. La cyberattaque le plus spectaculaire qui a eu lieu ces dernières années dans le monde maritime a touché l'armateur Maersk[44] ; en juin 2017 les systèmes informatiques de la compagnie ont été touchés par le raçonlogiciel NotPetya. L'attaque a paralysé le système informatique de Maersk durant dix jours et a fait baisser l'activité du groupe de 20 %.

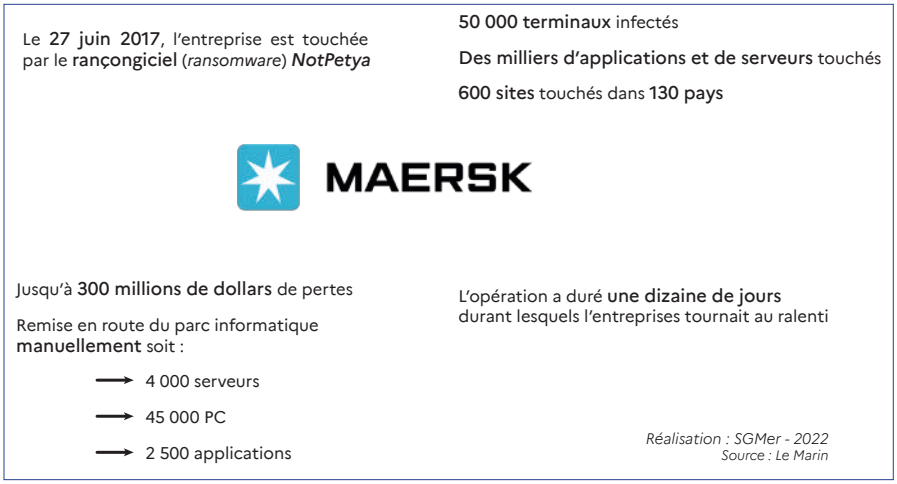


Figure n°5 : la cyberattaque de juin 2017 contre Maersk.

44 - Le Journal de la Marine Marchande, *AP Moller-Mærsk victime d'une cyberattaque*, 01 Janvier 2018. https://www.journalmarinemarchande.eu/mensuel/5081/tribune-libre/ap-moller-maersk-victime-dune-cyberattaque [Consulté le 02/06/2022].

Les tentatives de cyberattaque contre les compagnies maritimes sont devenues fréquentes. En 2018, Cosco Shipping a été touché par une cyberattaque qui a interrompu sa connexion internet dans ses bureaux en Amérique. Plus récemment les bureaux en Chine de CMA CGM ont été touché par le maliciel Ragnor Locker en septembre 2020. Cette attaque a causé la fermeture de tous les sites web externes de la compagnie.

2. La cybersécurité des infrastructures portuaires

A. Les vulnérabilités du secteur portuaire

Les infrastructures portuaires sont régulièrement touchées par des cyberattaques. Le développement de la mondialisation et l'accélération des échanges a rendu nécessaire l'usage des NTIC dans le secteur portuaire. Le rapport de l'ENISA « *Good practices for cybersecurity in the maritime sector* » de novembre 2019[45] met en exergue les vulnérabilités du secteur portuaire face aux cyberattaques.

45 - ENSIA, *Rapport Port Cybersecurity - Good practices for cybersecurity in the maritime sector,* november 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

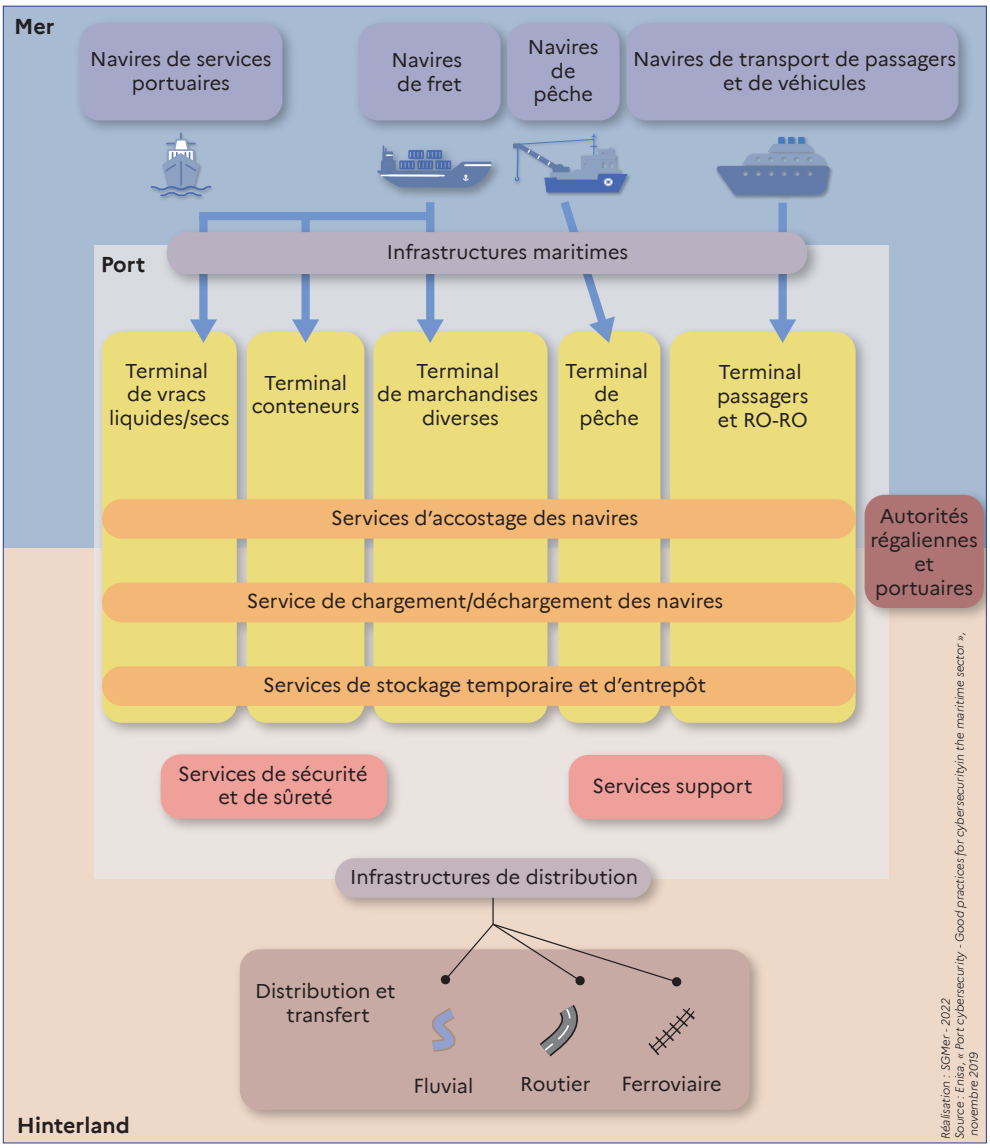


Figure n°6 : Les services et infrastructures portuaires pouvant être ciblés par des cyberattaques.

Les ports sont des espaces vulnérables car ils abritent de nombreux SI utilisés par des acteurs maritimes comme les compagnies de navigation, les agents maritimes, les acteurs du transport de fret ou de passager ou encore par les autorités locales, nationales ou européennes.

Le secteur portuaire abrite deux catégories de SI :

- Les systèmes d'information de gestion portuaire qui permettent l'exploitation des terminaux et le contrôle du trafic maritime ;
- Les systèmes d'échange de données qui constituent le point central de l'échange de données avec les compagnies maritimes.

Le dysfonctionnement de ces systèmes peut entraîner la paralysie du port et de ses opérations. Dès lors, les conséquences sur le transport maritime peuvent être assez lourdes ; un port peut perdre beaucoup d'argent à cause

de l'arrêt de ses opérations et voir sa réputation entachée à l'international, entrainant une perte de clients. Les clients touchés par l'arrêt des opérations, ou leur simple ralentissement, peuvent également être limité dans leurs activités commerciales.

Les systèmes informatiques des ports contiennent généralement des informations sensibles[46] qui peuvent être la cible des cyberattaques. De nombreux personnes travaillent au sein des systèmes portuaires, cela augmente la vulnérabilité des ports face aux attaques physiques comme le sabotage ou le vol de données.

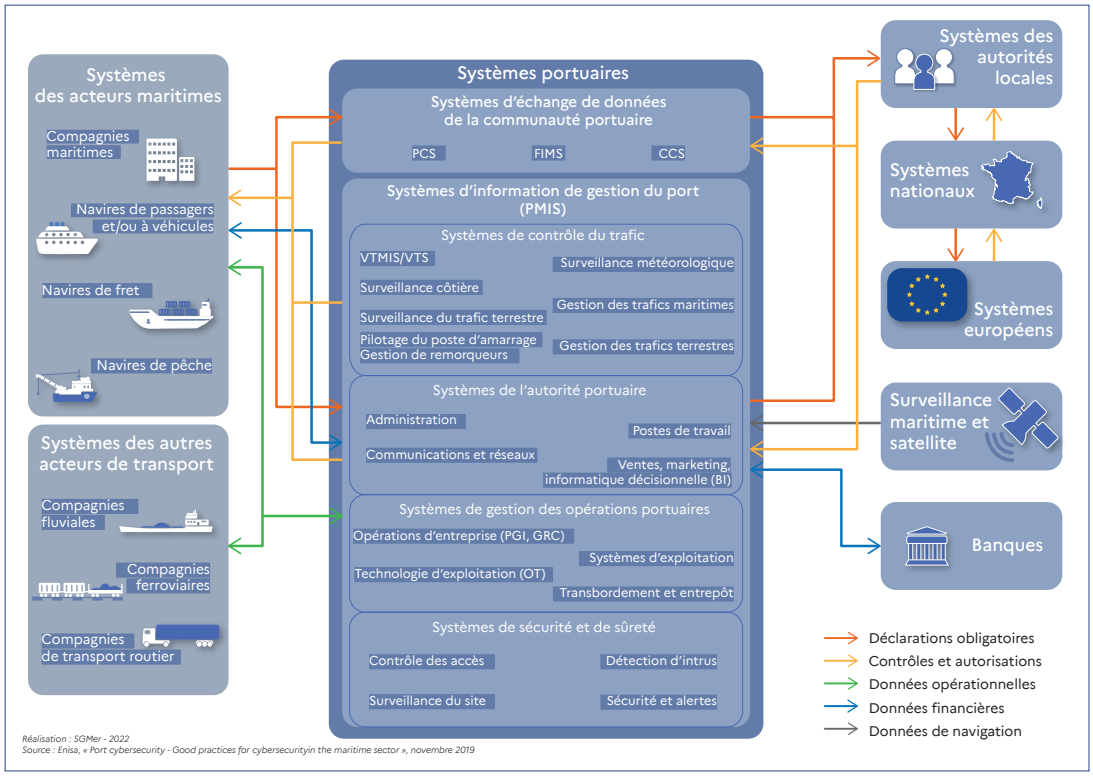


Figure n°7 : Les systèmes d'information (SI) portuaires.

B. La sécurisation du secteur portuaire

Les recommandations de l'ENISA

Dans son rapport de novembre 2019, l'ENISA recommande le déploiement d'une cybersécurité spécifique au secteur portuaire dont la gouvernance regrouperait l'ensemble des les acteurs impliqués dans des opérations portuaires (opérateurs, autorités portuaires, sociétés de transport maritime, pilote…).

46 - Elles peuvent être d'ordre personnel quand il s'agit de données sur les équipages ou sur les passagers, commercial avec la localisation et le contenu des conteneurs ou de l'ordre de la sécurité nationale avec les informations liées aux ports comme étant des atouts essentiels pour une nation.

Il est nécessaire que les ports renforcent leur capacité de réponse et de détection aux cyberattaques afin de réagir rapidement et de limiter les effets de l'attaque sur les SI. Ainsi, des systèmes d'alerte et de recherche d'indicateurs de compromission doivent être installés pour sécuriser le secteur.

La sensibilisation des acteurs à la cybermenaces est également important, cela passe notamment par l'apprentissage de la gestion des mises à jour, du renforcement des mots de passe ou encore le cloisonnement des réseaux.

Les recommandations de la DGITM

La DGITM[47] et les services de l'État français ont réalisé un guide de bonnes pratiques pour la cybersécurité dans le secteur portuaire[48]. Ce travail vise à proposer des recommandations et bonnes pratiques utiles à tous les acteurs des ports maritimes dans leur diversité pour que ceux qui le souhaitent, selon leurs capacités (organisationnelles, techniques, humaines, financières), puissent adapter leur action en matière de cybersécurité. Ce guide constitue la déclinaison française du guide de l'ENISA sur la cybersécurité dans les ports européens[49].

La stratégie du *smart port*

La stratégie du *smart port*[50] ou port intelligent, a été adoptée par les ports afin de concilier le recours aux données informatiques et la sécurité face aux menaces cyber. La compétitivité des ports repose en grandes partie sur la capacité de leurs SI à automatiser et traiter le flux d'informations liées aux marchandises, aux passagers et aux navires. Les SI portuaires permettent d'interconnecter tous les secteurs de l'activité du port et de coordonner de l'ensemble des opérations. Si l'interconnexion multiplie les risques de cyberattaques, elle peut aussi être utilisée pour élaborer une cybersécurité portuaire.

C'est la dynamique suivie par le port du Havre qui au travers de sa stratégie « *Smart Port City* »[51] vise à faire de la cybersécurité, un outil du développement de l'activité du port et de résilience. Cette stratégie a pour objectifs de susciter l'intérêt des acteurs de la sécurité en plaçant la cybersécurité sous l'angle de l'innovation et de la recherche. Les réflexions sur la protection des SI interconnectés contribuent à renforcer la compétitivité et la sécurité des ports.

47 - La direction générale des infrastructures, des transports et des mobilités (DGITM) prépare et met en œuvre la politique nationale des transports terrestres et fluviaux.

48 - DGITM, *Ports « cybersécurisés » Guide de bonnes pratiques pour la cybersécurité dans le secteur portuaire,* Juin 2021. http://www.port.fr/sites/default/files/fichiers/dgitm_-_guide_ports_cybersecurises_vd_-_diffusion_-_2021.pdf.

49 - ENSIA, *Rapport Port Cybersecurity - Good practices for cybersecurity in the maritime sector,* november 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

50 - La stratégie du *Smart Port* vise à renforcer la compétitive d'un port grâce à l'utilisation des technologies de l'information et du numérique (le *Big Data*, l'intelligence artificielle, la blockchain…). L'usage des nouvelles technologies permet de fluidifier le trafic maritime et de réaliser des économies d'échelle.

51 - Site internet du *Smart port City* du port Havre. https://www.lehavre-smartportcity.fr/ [Consulté le 07/06/2022].

IV. L'action de l'État

1. Une gouvernance de la cybersécurité

A. Le Conseil de Cybersécurité du Monde Maritime (C2M2)

La création du Conseil de cybersécurité du monde maritime en 2019 fait suite à la décision du CIMer 2018[52] de doter le monde maritime d'une structure de gouvernance et d'un centre de coordination pour faire face au risque cyber dans le secteur maritime. Le Conseil est un organisme de pilotage de la cybersécurité qui regroupe les acteurs français du maritime sous l'impulsion du Comité France maritime[53]. Le Conseil comprend quatre collèges : les opérateurs, les services de l'État, les industriels, les services des territoires. Sa gouvernance est assurée par un Comité exécutif présidé par le Secrétariat général de la mer qui se charge de la stratégie de communication vers des acteurs externes, du suivi des travaux menés et de la validation des projets initiés par des groupes techniques. Les groupes techniques réunissent des experts volontaires qui souhaitent travailler sur des sujets déterminés[54].

B. L'association France Cyber Maritime

France Cyber Maritime a été créée en 2020 suite à l'impulsion du CIMer 2018[55]. France Cyber Maritime est une association basée à Brest dont l'ambition est la promotion du développement de la cybersécurité maritime en France. L'association est organisée en trois collèges (le collège acteurs publics[56], le

52 - Site internet du Gouvernement, dossier de presse du CIMer 2018. https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2019/02/dossier_de_presse_-_cimer_2018_vf.pdf [Consulté le 07/06/2022].

53 - Le Comité France maritime est une instance de dialogue entre les filières de l'économie maritime et les acteurs publics.

54 - Les trois principaux sujets traités par les groupes de travail du C2M2 sont : l'élaboration d'indicateurs de suivi de la cybersécurité, le renforcement de la cybersécurité des navires autonomes, l'élaboration de dispositifs sectionnels de gestion de crise.

55 - La mesure 46 du CIMer souhaitait la mise en œuvre d'une Commission de cybersécurité préfigurant la création d'un centre national de coordination de la cybersécurité pour le maritime.

56 - Le collège est constitué de : l'Agence nationale de sécurité des systèmes d'information, Brest Métropole, le GIP ACYMA, la Région Bretagne, le Service Hydrographique et Océanographique de la Marine (SHOM).

collège utilisateurs[57], le collège solutions[58]), elle permet de faire le lien entre les opérateurs maritimes et portuaires ayant des besoins spécifiques en cybersécurité et des offreurs pouvant y répondre. Ainsi l'association contribue au développement d'une offre industrielle et technologique qui répond aux besoins des secteurs maritimes et portuaires. L'association mène également des actions de formation et de sensibilisation, notamment sur les bonnes pratiques à adopter en termes de cybersécurité.

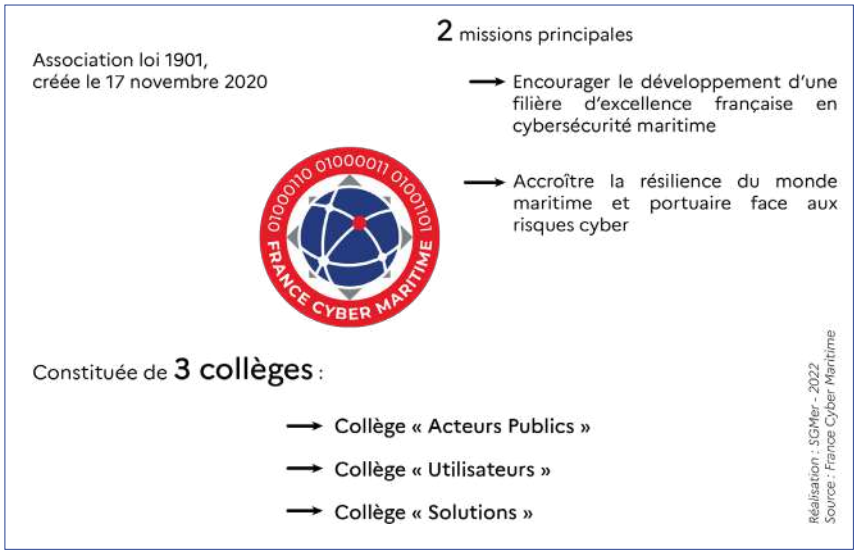


Figure n°8 : Présentation de France Cyber Maritime.

France Cyber Maritime a reçu le soutien financier de l'État[59] pour créer un Centre d'alerte et de réaction aux attaques informatiques maritime ; le M-CERT[60]. Le M-CERT est un centre de veille et d'alerte composé d'une équipe d'experts en sécurité informatique. Le Centre mène également des activités d'analyse afin d'anticiper le futurs risques cyber. Xavier Rebour le président de France Cyber Maritime présente le M-CERT comme « *un SAMU de la cybersécurité pour le monde maritime. Ses experts seront d'abord chargés de faire de la veille, de l'analyse de vulnérabilités et d'alerter les adhérents des menaces en cours. Cette première version du centre verra le jour avant la fin 2021. D'ici 2023, nous entendons aller plus loin, et créer une*

57 - Le collège est constitué de : Les Abeilles International, Alcatel Submarine Networks Marine, Armateurs de France, Bolloré Ports, Cerema, Compagnie Maritime Nantaise, le Cluster Maritime Français, CMA CGM, ELENGY, Fédération française des pilotes maritimes (FFPM), GAZOCEAN, GENAVIR, GICAN, GIE VIGIE Ports, Institut Français de Recherche pour l'Exploitation de la Mer (IFREMER), Naval Group, NEXEYA, Pôle Mer Bretagne Atlantique, Pôle Mer Méditerranée, PONANT, Port de Brest, Ports de la rade de Toulon, Seaowl Marine, Technopôle Brest Iroise.

58 - Le collège est constitué de : Adam Assurances, Alcyconie, Allentis, AMOSSYS, BESSE, CyWake, Défense Conseil International, DIATEAM, École Navale, ENSM, ENSTA Bretagne, Filhet-Allard Maritime, Fondation méditerranéenne d'études stratégiques (FMES), Gatewatcher, GLIMPS, HarfangLab, Holiseum, IMT Atlantique, Iot.bzh, KUB-CLEANER, Marlink, Pôle d'Excellence Cyber, Prorisk, SEKOIA, Semsoft, SourcITEC, Synacktiv, Thales, THALOS, Yes We Hack.

59 - Mer et Marine, *France Cyber Maritime va commencer à constituer l'équipe du CERT maritime*, Gaël Cogné, 4 juin 2021. https://www.meretmarine.com/fr/marine-marchande/france-cyber-maritime-va-commencer-a-constituer-l-equipe-du-cert-maritime [Consulté le 07/06/2022].

60 - *Maritime Computer Emergency Response Team.*

véritable hotline 24h/24 pour répondre aux incidents des acteurs du secteur »[61].

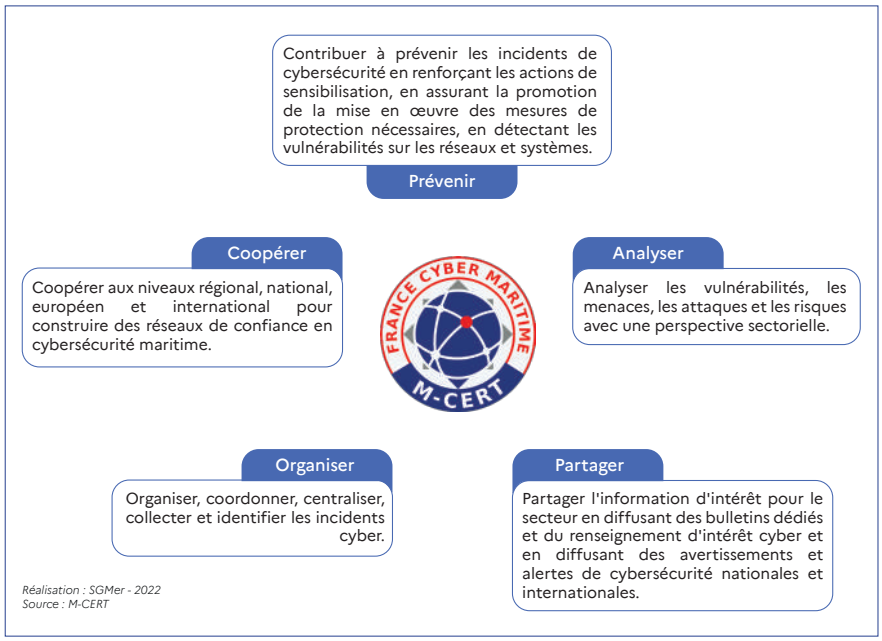


Figure n°9 : Les cinq missions de la *Maritime Computer Emergency Response Team*

2. Le développement de la cybersécurité

A. Le 4e programme d'investissement d'avenir (PIA4)

61 - Site internet de Goron, *Secteur maritime : la nouvelle association France Cyber Maritime fourbit ses armes contre les cybermenaces*, 16 février 2021. https://rendre-notre-monde-plus-sur.goron.fr/secteur-maritime-la-nouvelle-association-france-cyber-maritime-fourbit-ses-armes-contre-les-cybermenaces/ [Consulté le 07/06/2022].

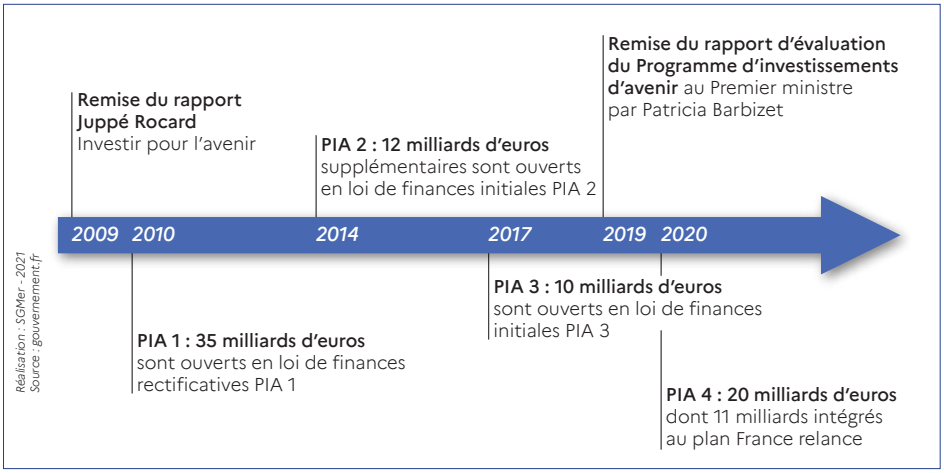


Figure n°10 : La décomposition du Programme d'Investissement d'Avenir (PIA).

Piloté par le Secrétariat général pour l'investissement (SGPI)[62], le Programme d'investissement d'avenir (PIA)[63] a pour objectif de financer des investissements prometteurs et innovants sur l'ensemble du territoire et dans des secteurs stratégiques identifiés.

Le PIA4 a été lancé en 2020 suite à la crise sanitaire du Covid-19. Le programme est doté de 20 milliards d'euros et s'étend sur cinq ans. Le PIA4 est novateur car il mêle investissements dirigés[64] et structurels[65]. Le PIA 4 possède un volet de « digitalisation et décarbonations des mobilités » visant à accélérer la transition vers une mobilité décarbonée et favoriser le développement d'une offre de mobilité, sûre, résiliente et accessible à tous. Ainsi, le PIA4 est investi sur les questions de cybersécurité. La PIA4 a également permis le déploiement du Grand défi Cyber[66] dont certaines innovations pourront s'appliquer au

62 - Crée en 2011 le Secrétariat général pour l'investissement (SGPI) est chargé, sous l'autorité du Premier ministre, de la mise en œuvre du Programme d'investissements d'avenir (PIA). Le Secrétariat assure également l'évaluation socio-économique des grands projets d'investissement public.

63 - Le Programme d'investissements d'avenir (PIA) a été créé en 2010 suite à la publication du rapport Juppé-Rocard de 2009 qui soulignait le manque de dispositif public en faveur de l'innovation. Le programme a été mis en place par l'État pour financer des investissements prometteurs et innovants sur l'ensemble du territoire et dans des secteurs stratégiques pour la France (transition écologique, compétitivité des entreprises, enseignement supérieur et recherche, souveraineté industrielle, économie numérique…) afin de permettre à la France d'augmenter son potentiel de croissance et d'emplois.
Le PIA intervient sur tout le cycle de vie de l'innovation (de l'émergence d'une idée jusqu'à la diffusion sur le marché du produit ou du service fini) et fait le lien entre la recherche publique et le monde de l'entreprise. Le PIA repose sur un double principe d'effet de levier et de partage des risques : l'investissement de l'État dans un projet d'innovation est la plupart du temps cofinancé par des partenaires privés ou publics.

64 - Financements destinés à répondre aux enjeux liés à la transition écologique.

65 - Financements visant à poursuivre et pérenniser certains projets soutenus par les PIA précédents.

66 - En partie financé par le PIA, le Grand Défi Cyber vise à soutenir les PME et les start-up française dans le développement d'innovation de ruptures. Le Grand Défi Cyber soutien trois thématiques d'innovation cyber : la protection des réseaux dynamiques, la protection des objets connectés, la protection des petites structures contre la cybercriminalité. 27 projets (16 PME et 11 start-up) ont été retenus lors de l'appel d'offre de 2020 pour un total de 15,9 milliards d'euros.

secteur maritime. À titre d'exemple IOT BZH l'un des lauréats du Grand défi Cyber, vise à mettre au point un conteneur sécurisé[67].

B. Les Comités interministériels de la Mer

Depuis quelques années, le Gouvernement, par des mesures prises durant les Comité interministériel de la mer (CIMer), soutient le déploiement d'une ambitieuse stratégie de cybersécurité maritime. Ainsi, le CIMer 2018 a permis la création du Centre national de coordination de la cybersécurité pour le maritime (C2M2)[68].

La nouvelle stratégie nationale portuaire[69] validée lors du CIMer 2021[70] met l'accent sur la transition écologique et numérique des ports maritimes. Afin d'allier cybersécurité et innovation, la nouvelle stratégie préconise notamment la création d'une communauté de responsables de la transformation digitale (« chief digital officers ») qui seront chargés d'animer la transformation numérique des grands ports maritimes sur ces deux volets. Cette communauté devra partager les expérimentations, initiatives et bonnes pratiques de certains grands ports maritimes dans le domaine de la cybersécurité pour permettre leur diffusion à l'ensemble des ports maritimes

Le CIMer 2022[71] a souligné l'importance des CCS (les systèmes portuaires d'information dédiés au suivi des marchandises) et demandé qu'une étude soit menée afin de mesurer les effets que pourrait générer une attaque cyber des CCS. L'étude sera menée par la DGITM et l'ANSSI.

67 - Communiqué de presse du Gouvernement, annonce des 27 lauréats du grand défi cyber (start-up et PME), 15 juin 2021. https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/06/20210604_communique_de_presse_laureats_aap_grand_defi_cyber_vdef.pdf [Consulté le 07/06/2022].

68 - Site internet du Gouvernement, *dossier de presse du CIMer 2018*. https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2019/02/dossier_de_presse_-_cimer_2018_vf.pdf [Consulté le 07/06/2022].

69 - La nouvelle stratégie nationale portuaire à horizon 2025-2050 a été adoptée par le Comité interministériel de la mer du 22 janvier 2021 et poursuit un objectif de reconquête de parts de marché et de développement économique des ports français.

70 - Site internet du Gouvernement, *dossier de presse du CIMer 2021*. https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/01/2021-01-22_dossier-presse-cimer.pdf [Consulté le 07/06/2022].

71 - Site internet du Gouvernement, *dossier de presse du CIMer 2022*. https://www.gouvernement.fr/sites/default/files/document/document/2022/03/dossier_de_presse_-_rapport_du_comite_interministeriel_de_la_mer_-17.03.2022.pdf [Consulté le 07/06/2022].

Conclusion

Avec la transformation numérique des navires et des infrastructures portuaires, la cybersécurité maritime devient un réel impératif. Si les acteurs majeurs (compagnies maritimes, grands ports) sont maintenant parfaitement conscients de l'impact considérable que des cyberattaques peuvent causer sur leurs SI, la prise de conscience de ces nouvelles menaces s'effectue progressivement chez les acteurs plus modestes, dont les moyens et les compétences informatiques sont plus limités. Aussi, la filière industrielle de la cybersécurité maritime civile reste encore embryonnaire même si elle peut s'appuyer sur de grands groupes matures dans le domaine tels que Naval Group. Or le secteur maritime est nécessaire au fonctionnement de l'économie puisque 90 % du commerce mondial s'effectue par voie maritime. Flottes et ports maritimes doivent donc absolument être protégés des cyberattaques, ce qui impose de protéger la chaîne complète des intervenants. Pour cela, depuis quelques années, l'État a remis au centre des enjeux économiques la thématique de la cybersécurité maritime. Le corpus juridique est en phase de consolidation et vise à mieux protéger les infrastructures et les activités existantes. Afin de développer au niveau national et internationale la cybersécurité, la France peut s'appuyer sur la compétence de l'ANSSI et, pour le monde maritime, compter sur de nouveaux acteurs, comme le C2M2 ou France Cyber Maritime.