ISEMAR
INSTITUT SUPÉRIEUR D'ÉCONOMIE MARITIME
NANTES - SAINT NAZAIRE

La cybersécurité un défi majeur pour le monde maritime

L'ère du numérique représente des opportunités en termes de sécurité, de performance économique et de monitoring environnemental pour le secteur maritime. De la navigation, à la propulsion, de la gestion du fret au contrôle du trafic maritime, les enjeux sont colossaux. Les cyberattaques deviennent de plus en plus courantes à mesure que la numérisation de nos activités progresse. Des vulnérabilités techniques connues et non corrigées, humaines au travers d'une non-acculturation à la menace cyber ou bien organisationnelles, existent à des degrés divers. L'interconnectivité de l'ensemble des acteurs ainsi que l'agrégation de services (smart port, smart ship, smart container, IA…) augmentent le risque de propagation de cyberattaques (rançongiciel, malware). L'impact peut être numérique, physique, financier, juridique et constituer une atteinte à la réputation de l'entité. Désormais, la sécurité des personnes, des biens et de l'environnement est également en jeu. Les trois plus grands armateurs mondiaux que sont, Maersk, MSC et CMA CGM ont été victimes de cyberattaques ces dernières années. Le secteur maritime devient le terrain de jeu de pirates informatiques professionnels organisés et dont les ressources ne cessent de croître. Leurs techniques sont de plus en plus sophistiquées. Leurs motivations sont diverses ; gangs criminels, activistes politiques, puissances étrangères et acteurs soutenus par l'Etat, groupes terroristes, et ce, d'autant plus dans le contexte géopolitique actuel très tendu. Comment le monde maritime appréhende-t-il les cyber-menaces?

Eléments de contexte

Les codes malveillants et rançongiciels sont les plus fréquents, devant les intrusions dans les réseaux. Le domaine de la logistique et de la chaine d'approvisionnement est le plus touché devant les armateurs et les ports. Les USA ainsi que la France sont les deux Etats ayant subi le plus d'incidents maritimes.

Volet navire

Les cyber-systèmes pour les navires ou les plates-formes offshores sont classés soit en IT (Technologies de l'Information) soit en OT (Technologies Opérationnelles). L'IT peut contenir toutes sortes de données non opérationnelles pour la conduite du navire, mais pour autant importantes, comme la liste d'équipage, la planification de la maintenance, les permis de travail, les manuels et certificats électroniques, la charte partie… L'OT est le support de toutes les fonctions opérationnelles du navire comme la navigation, la propulsion ou encore l'appareil à gouverner. Il comprend des systèmes d'information comme le GPS, l'ECDIS (*Electronic Chart Display and Information System*), le système de contrôle et d'acquisition des données en temps réel (SCADA), des automates et interfaces associés pour contrôler les machines embarquées, les enregistreurs de données, le positionnement dynamique, la stabilité du navire avec la gestion des eaux de ballasts… Une cyber-attaque sur l'OT est susceptible de mettre en danger navire et équipage.

Chaque armateur cherche à optimiser ses expéditions. L'analyse des données numériques représente un avantage concurrentiel et incite l'ensemble des acteurs à faire de même. Les Gouvernements, les organismes de règlementation ainsi que les exigences clients poussent également vers la voie de la traçabilité et du contrôle permanent qu'offre le numérique.

En France, la formation initiale des étudiants à l'ENSM intègre la cyber sécurité, depuis 2019 via un module de sensibilisation sur la réglementation et sur des scénarii d'attaques dans le maritime et le portuaire (prévention, diffusion des bons gestes…). Plusieurs élèves ont pu participer à des projets de recherche avec la création de scénarii de cyber-crises via le simulateur MARINS et la sécurisation de la norme S-100 (carte électronique pour la navigation), permettant ainsi d'éprouver la marétique et le facteur humain. En partenariat avec l'ENSTA, l'Ecole Navale [1] et l'IMT Atlantique un mastère spécialisé cybersécurité des systèmes maritimes et portuaires avait vu le jour. On peut regretter que ce dernier n'ait pas été reconduit cette année.

Volet portuaire

La révolution des "ports 2.0" s'est faite grâce aux fournisseurs de services numériques portuaires tels que le *Cargo Community System* (CCS) et le *Port Community*

1 L'Ecole Navale dispose d'un simulateur de recherche et de formation sur la cybersécurité maritime (cyber range-maritime) opéré par la chaire de cyberdéfense des systèmes navals.

System (PCS). Le CCS est un logiciel qui facilite le passage portuaire de la marchandise et simplifie les démarches administratives des professionnelles (armateurs, transitaires, agents maritimes, terminaux, autorités portuaires, douanes).
Le PCS est une solution numérique qui permet de planifier et d'organiser la gestion des escales. L'atteinte à l'intégrité ou la disponibilité du système de gestion de l'énergie électrique du port (Transformateurs, Générateurs, *Power Management Systems*) peut provoquer un dysfonctionnement de l'alimentation électrique ou un blackout mettant à l'arrêt l'activité portuaire (systèmes IT et OT, système de surveillance du trafic VTS, feux, écluses, ponts, grues, entrepôts réfrigérés, alimentation des conteneurs réfrigérés, alimentation des navires à quai, pompes, systèmes de sécurité et de sûreté, contrôle d'accès, portes automatiques). L'automatisation de portiques, les senseurs et caméras capables d'analyser les comportements, les difficultés de transit et la maintenance de manière apprenante, sont désormais une réalité.

La cybercriminalité dans le maritime
Plus les navires et les ports sont connectés plus la menace cyber évolue : panne de réseau, perte de données, perte de cargaison, escroquerie au bunkering, phishing, interférences du signal GPS, téléchargement de connaissement et détournement de conteneur.
En 2011, le port d'Anvers fut victime d'une cyber-attaque. Cette même année, *l'European Network and Information Security Agency* (ENISA) publiait un rapport alarmiste sur le niveau de sécurisation numérique du monde maritime. La cyberattaque mondiale NotPetya en 2017 a contaminé des milliers d'ordinateurs perturbant pendant des mois des multinationales et infrastructures critiques, comme les ordinateurs de contrôle du site nucléaire de Tchernobyl, les ports de Mumbai, d'Amsterdam, ainsi que les activités économiques de Maersk.
Le coût estimé serait supérieur à 10 Mds$. Bien que cette cyber attaque ait mené à une prise de conscience accrue de la menace cyber, cette dernière est aujourd'hui plus présente que jamais. Selon le rapport *Safety and Ships* 2023 d'Allianz le constat est inquiétant. 44% des professionnels du maritime ont fait l'objet d'une cyber-attaque au cours des trois dernières années et 1/3 des organisations n'ont pas de cyber plan (plan de reprise d'activité, plan de continuité d'activité) en cas d'attaque. Quatre professionnels sur dix estiment que leur entité n'a pas assez investi d'argent pour faire face à la menace cyber. La cyberattaque est fondée sur la détection et l'exploitation des vulnérabilités de la victime, il convient de renforcer les acteurs de "première ligne" de cette guerre de l'ombre. Pas seulement au niveau des fonctions RSSI (Responsable de la Sécurité des Systèmes d'Information) pour la plupart déjà confrontées aux cyberattaques, mais également depuis les directions générales, seules capables de donner au directeur des systèmes d'information (DSI), les moyens à la hauteur de l'enjeu et à forcer l'ensemble, notamment les opérateurs et utilisateurs finaux des SI à prendre en compte cette dimension.

Corpus réglementaires
A l'échelle internationale
Le risque cyber reste dans l'angle mort de la réglementation internationale, ne faisant l'objet que de recommandations très généralistes de la part de l'OMI.
Le Code ISPS (*International Ship and Port Facility Security*), instrument de référence en matière de sûreté maritime, prévoit ainsi dans sa partie facultative que "*l'évaluation de la sûreté du navire devrait porter sur les (...) systèmes de radio et télécommunications, y compris les systèmes et réseaux informatiques.*"
Consciente des enjeux, l'OMI au travers du Comité de Sécurité Maritime (MSC) a adopté en juin 2017 la résolution MSC 428(98) intitulée, *Maritime cyber risk management in safety management systems* qui reconnait l'urgence de sensibiliser le monde maritime aux cyber-risques. Cette résolution reste très généraliste et renvoie aux Etats membres la responsabilité d'en déterminer les conditions d'application. Elle s'adosse au Code International de gestion de la sécurité (Code ISM). C'est au travers de ce cadre règlementaire que les armateurs sont audités.
L'OMI a également publié en 2016 et 2017 des recommandations sur la gestion des cyber-risques maritimes[2] qui se déclinent en cinq étapes :

- Identifier : Définir les rôles du personnel et leurs responsabilités en matière de gestion des cyber-risques, identifier les systèmes et données sensibles.
- Protéger : Mettre en œuvre des processus de contrôle des risques, plans d'urgence, assurer la continuité des opérations.
- Détecter : Développer et mettre en œuvre des activités nécessaires pour détecter un cyber-événement.
- Répondre : Mettre en œuvre un plan pour développer la résilience et restaurer le système.
- Récupérer : Identifier les mesures de sauvegarde et de restauration du système.

[2] Circulaire révisée MSC Circ 1526 du 1er juin 2016 « Guidelines on maritime cyber management » et la circulaire MSC.1-FAL.1/Circ.3.

Ces circulaires renvoient elles aussi aux lignes directrices que peuvent émettre les Etats, les administrations du pavillon et les organismes professionnels du secteur maritime. En effet, parallèlement aux travaux de l'OMI, des associations maritimes internationales, des représentants d'armateurs (CLIA, Intertanko, Intercargo, Bimco), des sociétés de classification via l'IACS (*International Association of Classification Societies*), des assureurs[3] ainsi que des administrations étatiques comme l'USCG (*U.S Coast Guard*) éditent leurs propres guides d'hygiène informatique (architecture réseau sécurisée, contrôle d'accès, protection des données, évaluation et réponse aux incidents...).

L'Organisation internationale de la normalisation (ISO) dispose d'une série de normes qui complète les travaux sur la cybersécurité avec la norme ISO 28000 sur le management de la sécurité de la chaine d'approvisionnement, l'ISO 24060 (*Ships and marine technology Ship software logging system for operational technology*) et la norme ISO/IEC 27001 (*International standard for information security management systems* ISMSs) qui est la plus reconnue sur le plan international dans l'amélioration continue d'un système de management de la sécurité de l'information.

L'IACS émet des recommandations, qui pour certaines ont fait l'objet d'exigences unifiées minimales à l'ensemble des sociétés de classification IACS. Cela contribue à garantir que les nouveaux navires soient conformes aux dernières normes de la cybersécurité. Chaque membre reste libre de fixer des conditions plus strictes.

Ces travaux permettent d'homogénéiser le niveau de certification en matière de cyber-résilience des navires et de cybersécurité des systèmes et équipements embarqués (UR E22, UR E26 et UR E27). La standardisation à l'échelle internationale de la cybersécurité et son intégration dans la conception des systèmes du navire sont fondamentales.

A l'échelle européenne

La directive européenne 2016/1148 *Network Information Security* (NIS), entrée en vigueur en 2018 a été le premier cadre règlementaire européen destiné à assurer un niveau "*élevé commun de sécurité des réseaux et des systèmes d'information dans l'UE*", pour tous les modes de transports motorisés.

Des obligations sont désormais adressées aux Etats et aux opérateurs afin d'assurer une réponse unifiée à l'échelle européenne aux cyber-menaces.

La directive révisée NIS2 de 2022[4], prévoit que les Etats-membres puissent répondre aux incidents de sécurité informatique, avec la création d'une autorité nationale compétente en matière de réseaux et de systèmes d'information. Les Etats membres doivent coopérer et échanger des informations sur les menaces en cours. Ils doivent insuffler une culture de la sécurité dans les secteurs vitaux de l'économie qui dépendent fortement des TIC comme l'énergie, les transports, l'eau, les banques, les marchés financiers, la santé et le numérique. Les entreprises identifiées par les Etats membres comme entités essentielles ou importantes (EE/EI) dans ces secteurs, devront prendre des mesures de sécurité appropriées et informer les autorités nationales compétentes des incidents graves.

Les compagnies de transport et les gestionnaires de ports sont soumis à ces dispositions. Des mesures techniques, organisationnelles incluant fortement le facteur humain, sont des leviers d'action privilégiés de la cybersécurité. Cette nouvelle mouture plus exigeante doit être transposée dans le droit national au plus tard fin 2024. Elle prévoit pour les entités régulées de lourdes amendes, voire le retrait de l'autorisation d'exploitation en cas de non-conformité à la NIS2. L'obligation réglementaire oblige les EE/EI à investir et permet de mettre tout le monde sur un même pied d'égalité. Ces opérateurs sont également garants de la cybersécurité de leurs fournisseurs ainsi que de l'ensemble de la chaine d'approvisionnement, cela aura un impact contractuel.

La directive rend obligatoire le signalement d'incidents dans les 24h et souhaite ainsi favoriser le partage d'informations entre Etats-membres et mieux déterminer si cet événement aura un impact transfrontalier. Ce n'est qu'en partageant les informations et les expériences que l'industrie pourra créer des normes et les meilleures pratiques en matière de cybersécurité. France Cyber Maritime (le M-CERT) tient une base de données publique ADMIRAL des incidents de cybersécurité connus et publics ayant touché le secteur maritime au sens large et à l'échelle internationale.

A l'échelle française

La loi de programmation militaire (LPM) est un plan stratégique de défense. Elle est votée tous les 5 ans. Elle désigne près de 250 opérateurs d'importance vitale (OIV), privés et publics indispensables au bon fonctionnement de la Nation. Les OIV ont notamment des obligations légales concernant la cybersécurité.

[3] Guide pour lutter contre la cyber attak "*guide to cyber – risk: managing the impact of increasing inter connectivity* "publié par *Allianz Global Corporate & Speciality* (AGCS) sept 2015.

[4] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022.

La règlementation nationale intègre les exigences spécifiques du code ISPS dans la division 130 annexée à l'arrêté du 23 novembre 1987 modifié relatif à la sécurité des navires et à la prévention de la pollution. L'article 130.28 dispose pour les navires : "*III Prise en compte du cyber risque : Toute compagnie soumise à l'obligation de détenir un document de conformité s'assure que les cyber-risques sont convenablement incorporés dans son système de gestion de la sécurité. A l'occasion des audits menés en vue de la délivrance ou du renouvellement du document de conformité et en application de la résolution OMI MSC 428(98), la compagnie expose à minima les dispositions prises vis-à-vis :*

a) De sa politique générale de cybersécurité ;
b) De la conduite et de la mise à jour de son analyse de risques, incluant un inventaire des systèmes et des procédures existantes ;
c) Des procédures techniques, humaines et organisationnelles mises en place ;
d) Des procédures de suivi au quotidien ;
e) Des procédures d'alerte et de gestion de crise."

Tout comme en matière de respect des normes de sécurité, de sûreté, des normes environnementales et sociales, la cybersécurité rentre dans le giron des Centres de sécurité des Navires (CSN). Au regard de la résolution MSC (428)98, les agents ne contrôlent pour le moment que les sièges sociaux des compagnies maritimes via des audits. Le manque de moyens, de temps et de compétences spécifiques affecte la capacité de l'administration du pavillon à faire une analyse fine et précise de cette question.

Face à ces menaces, les administrations concernées (SGMer, DGAMPA, DGITM, ANSSI), le secteur maritime et portuaire et le secteur de la cybersécurité se sont organisés, en créant le Conseil Cyber du Monde Maritime (C2M2) en 2019, dont les travaux ont suivi deux orientations. La première est l'analyse macro des risques et des scénarii d'attaques possibles. Cette identification des vulnérabilités permet de prioriser les actions à mener. La seconde est l'adoption en 2021 d'une cyber-stratégie du monde maritime, identifiant lesdites actions. Avec le soutien de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et sous l'impulsion du SGMer a été créée en 2020, l'association France Cyber Maritime qui a pour vocation de créer des synergies entre le secteur maritime et le monde cyber.

Elle apporte une expertise en matière de cybersécurité et une assistance en cas d'incident et contribue ainsi au renforcement de la résilience du secteur. France Cyber Maritime opère le M-CERT (*Maritime Computer Emergency Response Team*), un centre national dédié à la veille, à l'analyse et au partage des informations anonymisées relatives à la cybersécurité maritime et portuaire (suivi et actualisation des menaces, des vulnérabilités, des incidents…). L'association s'articule autour de trois collèges, acteurs publics (agences de l'Etat, Ministère, collectivités territoriales), utilisateurs (armateurs, ports, pêche) et solutions (matériel, audit, assurance, …).

L'acculturation au cyber-risque est fondamentale que ce soit à terre ou en mer. Comme pour d'autres risques, la logique prédominante est celle du renforcement de la prévention avec une politique d'investissements de longs termes sur les volets techniques et humains, et la couverture des risques subsistants par l'assurance.

Risque cyber et assurance

Il existe une logique d'exclusion du risque cyber par les assurances maritimes sur le plan international. Au regard des besoins du marché, la cyber-assurance s'est fortement développée ces dernières années via des polices d'assurance spécifiques, même si elles se sont révélées à perte pour les assureurs. En 2020, les assureurs ont perçu 130 M€ de primes pour 250M€ de sinistres couverts.

Ce risque reste difficilement appréhendé à la fois dans sa forme, mais surtout dans ses répercussions économiques en particulier en cas de perte de revenu due à un arrêt d'activité, d'où une montée en exigence dans la sélection des risques et l'application de majorations tarifaires à la fois sur les primes et les niveaux de franchises. En 2020, pour 1€ de prime versé, ce sont 10€ de garanties qui sont couverts par l'assurance cyber. La cyber-assurance étant un produit encore récent, il n'existe pas pour le moment de véritable standard de marché. Elle se décline en quatre piliers : Prévention, assistance (expert cyber /système, conseiller juridique/ communication), couverture des opérations (perte d'exploitation), couverture des responsabilités (coût des recours et dommages subis par des tiers). La police d'assurance doit véritablement s'ajuster aux besoins de l'entité. Le recours à un courtier pour comparer les offres est utile.

La question n'est plus comment, ni quand une cyber-attaque va se produire, mais plutôt, serai-je assez résilient pour faire face à celle-ci ? Les enjeux de la cybersécurité sont prégnants, l'intelligence artificielle, les drones maritimes et les navires autonomes sans équipage vont faire évoluer les pratiques de demain ainsi que le droit.

Camille VALERO

Avec le concours de la DGAMPA, de France Cyber Maritime ainsi que de Béssé Assurances

Octobre 2023 – ISSN : 1282-3910 – dépôt légal : mois en cours
Directeur de la rédaction : Paul Tourret – ISEMAR (droits réservés)