France Cyber Maritime : pour un monde maritime numérique plus sûr

Xavier Rebour
Contre-amiral (2S)
Directeur de France Cyber Maritime

Le 27 juin 2017, la compagnie danoise Maersk, l'un des leaders mondiaux du transport maritime, est victime d'une cyber-attaque d'une ampleur inégalée. Le ver informatique NotPetya neutralise en quelques minutes 4 000 serveurs et 45 000 ordinateurs de l'entreprise à travers le monde. 20 % de la capacité mondiale du transport maritime est à l'arrêt total. Le retour à la normale prendra plusieurs semaines, pour un coût pour Maersk estimé à 300 millions de dollars. Si cette attaque a marqué les esprits par son ampleur et ses conséquences, elle est loin d'être un évènement isolé. Plus d'une centaine d'incidents ayant touché le monde maritime et portuaire ont été recensés au cours des 13 dernières années. Il s'agit vraisemblablement de la partie émergée de l'iceberg, la majorité des incidents restant non détectés ou non déclarés.

Quelles menaces à l'encontre du monde maritime ?

Les données numériques sont soumises à plusieurs types de menaces, plus ou moins visibles. La menace la plus prégnante est la cybercriminalité, aux modes d'action variés selon la technicité des attaquants, individus isolés ou groupes criminels organisés. Le « *rançongiciel* », logiciel malveillant qui chiffre les données d'un utilisateur et qui nécessite une clé de déchiffrement contre

France Cyber Maritime : pour un monde maritime numérique plus sûr

rançon, en est la manifestation la plus fréquente et la plus médiatisée. L'activité de la victime est à l'arrêt ou fortement perturbée tant que la rançon n'est pas payée ou que les mesures de sauvegarde n'ont pas été mises en œuvre. Les attaques par rançongiciels sont souvent couplées à un vol de données donnant lieu à une deuxième extorsion ou une revente dans des réseaux criminels. En 2020 et 2021, de nombreux opérateurs maritimes et portuaires, dont plusieurs français, en ont été victimes. La cybercriminalité compte aussi de juteux trafics sur l'internet caché (le « *dark web* »), où la vente de données volées, de codes d'accès aux réseaux, de logiciels malveillants « clés en main » sont sources de profits illégaux considérables.

Les données numériques des États, des organisations et des entreprises peuvent également être victimes d'espionnage. Par nature insidieux, discret et de long terme, le cyber-espionnage est perpétré par des organisations structurées, étatiques, paraétatiques voire privées, à des fins politiques, stratégiques, militaires ou économiques. En novembre 2018, un chantier naval australien[1] qui conçoit des navires de combat pour la *Royal Australian Navy* et l'*US Navy* a été victime d'une intrusion informatique et a subi un vol de données.

Aussi le fait de groupes étatiques ou paraétatiques, mais aussi criminels ou terroristes, le sabotage par voie numérique est une menace réelle. La mise hors service des centrifugeuses iraniennes par le ver Stuxnet en 2010 reste dans les mémoires. Plus récemment, le port iranien de Shahid Rajaei[2] dans le détroit d'Ormuz aurait été victime d'un acte de cyber-sabotage en mai 2020, probablement perpétré par un pays du Proche-Orient.

Par ailleurs, des attaques numériques peuvent être perpétrées à des fins d'atteinte à l'image, de propagande, de désinformation, de manipulation de l'opinion. L'image de l'Organisation Maritime Internationale[3] (OMI), victime d'une cyber-attaque en septembre 2020, a été manifestement écornée, quelques semaines avant la mise en application le 1er janvier 2021 de sa directive MSC 428(98) relative à la prise en compte de la cybersécurité dans le système de gestion de la sécurité des navires (*Safety Management System*).

Plus spécifiques au secteur maritime, des opérations de brouillage et de falsification des systèmes GNSS[4] et AIS[5] sont possibles, pour perturber la navigation dans des zones particulières ou masquer des activités illégales ou inamicales. De telles actions ont déjà été observées en 2020 en Méditerranée orientale, en mer Noire et en mer de Chine.

1. *https://safety4sea.com/australian-defense-shipbuilder-austal-hit-by-cyber-attack/*
2. *www.zdnet.com/article/iran-reports-failed-cyber-attack-on-strait-of-hormuz-port/*
3. *https://gcaptain.com/international-maritime-organization-hit-by-cyber-attack/*
4. *GNSS : Global Navigation Satellite System, acronyme rassemblant les systèmes de positionnement, de navigation et de temps par satellites, tel le GPS américain, GALILEO européen et GLONASS russe.*
5. *AIS : Automatic Identification System. Système de diffusion radioélectrique d'informations concernant un navire : identité, position, route, vitesse, cargaison, trajet...*

Enfin, n'occultons pas les risques accidentels qui peuvent compromettre la sécurité des données, l'environnement maritime étant un milieu potentiellement hostile.

Les enjeux de la numérisation du secteur maritime et portuaire

Le monde maritime et portuaire s'est engagé depuis quelques années dans une transformation numérique sans précédent. Si la numérisation améliore les performances et la compétitivité du secteur, elle apporte de nouvelles vulnérabilités pouvant être exploitées par des organisations criminelles ou des États. Même si par de nombreux aspects, navires et ports peuvent s'apparenter à d'autres secteurs industriels, le secteur maritime et portuaire présente des besoins particuliers en matière de cybersécurité. Il met en effet en œuvre des équipements propres et opère dans des conditions d'exploitation et d'environnement spécifiques.

Le secteur maritime et portuaire dispose d'une part de systèmes d'information spécifiques dits « *Information Technology* », destinés à traiter les informations nécessaires à l'exploitation du navire ou du port : cartographie numérique (ECDIS[6]), AIS, systèmes de navigation par satellites (GNSS), communication par satellite, systèmes de gestion du port et du fret (PCS[7], CCS[8])… D'autre part, des systèmes numériques dits « *Operational Technology* » commandent les équipements industriels spécifiques : manœuvre du navire, gestion de la propulsion, des auxiliaires, de la sécurité, des pompes, vannes, grues et portiques. Sur des navires ou au sein d'installations portuaires au long cycle de vie, ces systèmes hétérogènes au cycle de vie plus court sont souvent mis en place en couches successives, par des constructeurs et des intégrateurs multiples, posant des problèmes de cohérence, de vue d'ensemble et de mise à jour.

Nombre de ces systèmes à bord des navires sont connectés par liaisons satellites, afin de les alimenter en données opérationnelles, permettre des opérations de contrôle et de télémaintenance. Portes d'entrée pour des actes de malveillance numérique, ces mêmes liaisons satellites rendent difficiles une surveillance des systèmes informatiques ou une intervention à distance en cas d'incident cyber, en raison d'une bande passante limitée, un temps de latence important et un coût élevé. Dans un port, la multiplicité des acteurs ayant accès aux systèmes pour assurer la bonne fluidité des activités portuaires complexifie la sécurisation numérique de l'ensemble.

Enfin, en matière de ressources humaines, les compétences spécifiques en cybersécurité maritime sont encore à développer et les équipages optimisés des navires ne comportent pas d'informaticien, encore moins d'expert en

6. *ECDIS : Electronic Chart and Display Information System*
7. *PCS : Port Community System*
8. *CCS : Cargo Community System*

France Cyber Maritime : pour un monde maritime numérique plus sûr

cybersécurité. Avant même de disposer d'expert, il convient de sensibiliser et former tous les utilisateurs de systèmes numériques maritimes et portuaires, du capitaine au matelot, du commandant de port au manutentionnaire.

Les risques et leur perception par le secteur maritime et portuaire

Les risques d'une cyber-attaque à l'encontre d'un navire ou d'un port sont multiples et leurs conséquences financières et parfois physiques potentiellement graves, avec des répercussions en cascade. En mer, la sécurité de la navigation peut être engagée, tout comme la sécurité du navire lui-même. La perturbation des mouvements des navires, des passagers, du fret, des services et des équipements, tout comme l'atteinte à la sécurité et à la sûreté peuvent conduire à la paralysie d'un port, entraînant des congestions à terre comme en mer, des pertes financières considérables et d'éventuels accidents. Les crises subies par Maersk et d'autres opérateurs maritimes et portuaires ces dernières années ont mis en lumière ces risques, ainsi que les conséquences dévastatrices sur le commerce mondial dépendant à 90 % du transport maritime. Aucun acteur de ce secteur critique pour l'économie française ne peut aujourd'hui s'estimer à l'abri.

La prise de conscience de la menace et des risques par les opérateurs maritimes et portuaires progresse. Mais la mise en place d'une politique de cybersécurité se heurte souvent à un manque de moyens, une gestion conjoncturelle des priorités ou encore un découragement face un domaine inconnu et jugé réservé aux experts. Il existe ainsi de grandes disparités entre les différents acteurs en matière de prise en compte de la cybersécurité. Si les grandes compagnies maritimes et les grands ports maritimes peuvent mettre en place une organisation, du personnel et des mesures adaptées, les opérateurs plus modestes manquent de compétences et de moyens, ou se pensent à l'abri en raison de leur taille ou de leur moindre visibilité. Les armateurs sont en particulier dans l'obligation depuis le 1er janvier 2021 de prendre en compte la cybersécurité dans leur système de gestion de la sécurité relevant du code ISM[9], en application de la directive MSC 428(98) de l'Organisation Maritime internationale (OMI). Les plus petites compagnies maritimes sont souvent démunies face à la mise en place de cette directive et ont besoin d'être accompagnées.

La genèse de France Cyber Maritime

C'est face à ces constats que la France décide en 2018 de prendre en compte la menace cyber à l'encontre du secteur maritime et portuaire, comme elle l'a déjà fait pour d'autres secteurs vitaux pour son fonc-

9. *ISM :* International Safety Management*, code international de gestion de la sécurité pour l'exploitation des navires.*

tionnement et son économie. Aussi le Comité Interministériel de la mer (CIMer) du 15 novembre 2018 décide-t-il par sa mesure 46 « *la création d'une commission cybersécurité et la préfiguration d'un centre national de coordination de la cybersécurité pour le maritime* ».

Le Conseil Cyber du monde Maritime (C2M2) voit le jour en novembre 2019. Présidé par le Secrétaire général de la mer avec pour vice-président le directeur général de l'Agence nationale de la sécurité des services d'information (ANSSI), il réunit dans un cadre public/privé administrations traitant des questions maritimes et opérateurs des secteurs maritimes, portuaires et de la cybersécurité. Il se donne pour mission de définir la politique et la stratégie française en matière de cybersécurité maritime.

Dès son instauration, le C2M2 décide la mise en place d'un groupe de travail afin de définir l'objet et les missions du futur centre de coordination de la cybersécurité pour le maritime. Ce groupe, piloté par le SGMer, rassemble les premiers acteurs publics et privés volontaires du domaine et reçoit le soutien technique de l'ANSSI. De nombreux opérateurs privés et acteurs territoriaux affichent par la suite officiellement leur soutien au projet.

Parmi les contributeurs aux travaux figure en particulier Brest métropole, qui s'est portée officiellement candidate pour accueillir le futur centre dès juillet 2019. La cité du ponant fait en effet valoir que la pointe de la Bretagne dispose d'un écosystème complet favorable au développement national de l'activité du centre : base navale et port civil, haut lieu des sciences et technologies de la mer, siège de nombreux acteurs académiques et industriels du maritime et de la cybersécurité. L'association loi 1901 France Cyber Maritime est ainsi créée à Brest le 17 novembre 2020, après que ses statuts aient été validés par le SGMer.

Fédérer pour créer une filière d'excellence et anticiper la menace

France Cyber Maritime a pour missions de contribuer au développement d'une filière d'excellence française en cybersécurité maritime en fédérant les acteurs du domaine, mais aussi d'opérer un *Maritime Computer Emergency Response Team* (M-CERT), centre national de veille, d'alerte et de recueil des incidents cyber pour le secteur. L'association fédère au sein de trois collèges acteurs publics, opérateurs maritimes et portuaires et offreurs de solutions de cybersécurité.

Le collège « acteurs publics » a vocation à accueillir les administrations et agences de l'État concernées et les collectivités territoriales littorales de métropole et d'outre-mer. Le collège « utilisateurs » ambitionne de regrouper les opérateurs des secteurs maritime et portuaire : compagnies maritimes, armateurs, ports de commerce, de pêche et de plaisance, chantiers navals, opérateurs *offshore* du pétrole, du gaz, des énergies marines renouvelables, des câbles sous-

France Cyber Maritime : pour un monde maritime numérique plus sûr

marins... Enfin le collège « solutions » héberge des offreurs de solutions de cybersécurité adaptées au secteur : entreprises, chaires industrielles, établissements d'enseignement et de recherche, pôles d'excellence, organismes de certification, courtiers en assurance maritime…

France Cyber Maritime accueillera progressivement de nouveaux membres, de manière contrôlée, afin d'étendre ses compétences et son maillage des secteurs maritime, portuaire et de la cybersécurité sur l'ensemble du territoire national.

Des solutions en cybersécurité adaptées aux besoins

La fédération des écosystèmes maritime et cybersécurité a pour objectif de créer une expertise française en matière de cybersécurité dédiée au monde maritime et portuaire, en développant des services qui répondent aux besoins de la filière. La collaboration au sein de France Cyber Maritime des opérateurs maritimes et portuaires, ayant des besoins spécifiques en cybersécurité, et des offreurs de solutions en cybersécurité, est de nature à développer cette expertise. La valeur ajoutée de l'association sera d'animer cette collaboration grâce à son équipe opérationnelle resserrée, composée de chargés de projets assurant le lien et structurant les échanges entre les différents acteurs.

Cette collaboration permettra d'une part la co-construction d'une offre de produits et services adaptée au secteur : analyse de la menace et renseignement cyber, surveillance des réseaux, sensibilisation, formation et entraînement, audit, conseil et mise en conformité, maintien en condition de sécurité.

Elle se concrétisera d'autre part par une activité de recherche et développement (R&D) et de soutien à l'innovation. Cette activité réunira autour de projets collaboratifs opérateurs maritimes, opérateurs de cybersécurité et établissements de recherche afin de mettre en œuvre des solutions innovantes adaptées aux besoins de la filière.

France Cyber Maritime participera également aux travaux nationaux de réglementation, certification et labellisation en la matière, en liaison avec les administrations et organismes concernés. Elle contribue déjà à développer et promouvoir l'excellence française en cybersécurité maritime, en particulier par les actions de communication, d'animation et de valorisation, en France comme à l'international.

Anticiper la menace et assister les victimes de cyber-attaques

Une plus grande résilience du monde maritime et portuaire passe par une capacité à anticiper la menace et à assister les victimes de cyber-attaques. C'est la mission du M-CERT, *Maritime Computer Emergency Response Team*. Composé d'une équipe d'experts en analyse de la menace et de

gestion de crise cyber pour le maritime, ce centre à vocation nationale implanté à Brest est en premier lieu chargé de la veille et l'analyse de la menace et de la diffusion de bulletins d'information et d'alerte, afin de permettre aux opérateurs maritimes et portuaires d'être alertés et d'anticiper les attaques. Il émet un bulletin mensuel d'informations destinés aux adhérents, qui décrit les incidents concernant le secteur maritime et portuaire survenus dans la période, détaille les menaces et les modes d'action des attaquants, informe sur les vulnérabilités identifiées sur des logiciels ou des équipements spécifiques au secteur, et préconise des mesures de prévention et de protection à mettre en œuvre. Ce bulletin comporte quatre niveaux de technicité[10] permettant une lecture et une appropriation par tous les destinataires, quel que soit leur niveau de maturité en cybersécurité. Le petit armateur sans service informatique bénéficiera d'informations de bonnes pratiques et de prévention, le grand opérateur maritime disposant d'experts en cybersécurité y trouvera quant à lui des données techniques très précises permettant de configurer ses systèmes de défense et de se prémunir contre certaines attaques.

Le M-CERT est ensuite chargé de recueillir les incidents, afin d'enrichir ses connaissances, affiner ses analyses et partager les alertes avec l'ensemble du secteur. Agissant comme tiers de confiance, il garantit strictement l'anonymat aux victimes qui lui reportent leurs incidents, ne diffusant de l'évènement que des données génériques non attribuables permettant de prévenir l'occurrence d'un incident similaire chez d'autres acteurs du secteur. Il rejoindra en 2022 l'Inter CERT-FR, le réseau des CERT français, fort d'environ 50 membres, dont le CERT-FR, centre de l'ANSSI chargé de la gestion des incidents de cybersécurité de l'État et des opérateurs d'importance vitale (OIV). CERT sectoriel national, il se coordonnera en particulier avec les CERT généralistes régionaux qui vont se mettre en place progressivement sous la tutelle des conseils régionaux, afin de veiller à la complémentarité et établir des collaborations. Ce cercle de confiance permettra des échanges opérationnels et techniques privilégiés, en toute confidentialité et de manière anonyme, afin de partager l'état de la menace entre différents secteurs. France Cyber Maritime a de plus établi des conventions de collaboration respectivement avec la Marine nationale et la Gendarmerie maritime, fixant ainsi un cadre à des échanges sur des thématiques duales ou judiciaires. Enfin, des premiers contacts bilatéraux sont déjà engagés avec des organismes de pays alliés traitant des questions de cybersécurité maritime.

Dans le cadre de sa progression sur trois ans, accompagné par l'ANSSI, le M-CERT offrira à terme une assistance aux victimes : qualification de l'incident, prise des premières mesures d'urgence, mise en relation avec des opérateurs

10. *Fondation, intermédiaire, avancé, renforcé.*

France Cyber Maritime : pour un monde maritime numérique plus sûr

de cybersécurité de proximité qualifiés pour traiter l'incident, coordination avec les différents intervenants et les services compétents.

Solidarité et confiance

Cette première année de mise en place et de fonctionnement de France Cyber Maritime a mis en lumière l'immensité des besoins. L'engagement des membres fondateurs et le financement initial accordé par l'ANSSI dans le cadre du volet cybersécurité de France Relance ont donné une impulsion initiale à cette initiative ambitieuse. France Cyber Maritime doit à présent affronter trois enjeux pour enclencher un cercle vertueux. Elle doit tout d'abord se mettre en capacité de remplir les missions qui lui sont confiées, répondre aux attentes de ses adhérents, développer les services à leur profit, et pour cela renforcer son organisation et son fonctionnement. Forte de premiers résultats concrets, elle pourra ensuite rayonner et convaincre de la pertinence de la démarche pour rallier progressivement le plus grand nombre d'acteurs, dont certains font face à d'autres priorités, sont indécis ou encore minimisent la menace. Elle pourra enfin consolider et pérenniser ses ressources sur le long terme dans un partenariat public/privé au bénéfice de la sécurité numérique de secteurs stratégiques pour la souveraineté et l'économie française.

Face à l'ampleur des risques et des menaces cybernétiques à l'encontre des secteurs maritimes et portuaires, la défense ne pourra être que collective. Fruit d'un partenariat public/privé, mue par un esprit de service d'utilité publique, France Cyber Maritime a l'ambition de créer une communauté alliant la solidarité des gens de mer et la confiance numérique propre à la cybersécurité. L'association compte à ce jour plus de 40 adhérents, emblématiques du monde maritime et de la cybersécurité. Elle accompagne déjà des opérateurs maritimes dans le renforcement de leur cybersécurité et va poursuivre, dans les mois à venir, le développement de ses services. Le M-CERT a démarré la diffusion de bulletins d'information et d'alerte et va poursuivre sa progression. La fédération de cette communauté solidaire et de confiance est en marche. Enclenchons maintenant le cercle vertueux.