Pandémie oblige, l'étape normande du Tour de France Cyber, les Rencontres de la Cybersécurité Normandie du CyberCercle, ont eu lieu le 10 décembre 2020 en distanciel. Ce qui n'a pas empêché une grande qualité d'échanges sur un sujet aussi critique qu'essentiel à l'activité économique mondiale.

Elles avaient pour fil rouge la cybersécurité maritime et portuaire, autour du projet de Smart Port City du Havre, projet structurant d'avenir soutenu par HAROPA - Port du Havre et la communauté urbaine Le Havre Seine Métropole.

Un trafic vital, mais de plus en plus vulnérable aux attaques cyber

Baptise MORAND, Directeur Général d'HAROPA - Port du Havre, a souligné en ouverture l'importance de la filière maritime dans les échanges mondiaux : le trafic maritime mondial représente à lui seul près de 80% des échanges commerciaux au niveau mondial.

L'essentiel du commerce mondial passe maintenant par ces forteresses flottantes, dont la pandémie a accru le rôle avec le nombre de produits manufactures commandés sur des sites marchands. Or, les conditions maritimes (phénomènes météos extrêmes de plus en plus fréquents), mais aussi l'importance la surface d'attaque que constitue le trafic maritime mondial au niveau cyber, due à la digitalisation accrue des bâtiments, des infrastructures portuaires et de l'ensemble de la chaine logistique rend ce domaine très sensible.

Comme l'a rappelé Baptise MORAND, *« l'incident heureusement maitrisé qui a eu lieu en septembre 2020 contre l'armateur CMA CGM, le premier armateur français, vient à point nommé pour rappeler la sensibilité de ce domaine stratégiques aux attaques cyber »*. Cette attaque partie du système informatique de réservation de fret en direction de la Chine, dont le mode opératoire est passé par un ransomware et l'action de l'organisation pirate Ragnar Locker aurait coûté, selon le site du journal de la marine marchande (https://www.journalmarinemarchande.eu/actualite/shipping/peril-informatique-apres-cma-cgm-lomi plus de 2 milliards de dollars.

Michel SEGAIN, Président de l'Union Maritime et Portuaire, a d'entrée appuyé sur l'importance de l'enjeu : *« notre cybersécurité est un enjeu de défense nationale, et il est de notre devoir de tout mettre en œuvre pour coordonner de la manière la plus efficace possible la prévention des risques, l'identification et le traitement de nos vulnérabilités, la coordination de nos actions en cas d'attaques ».*

Il rappelle également que « *leurrer une cargaison, un système de navigation (AIS, GNSS) est possible, et les bâtiments sont devenus tellement informatises qu'ils deviennent eux aussi la proie d'attaques informatiques d'ampleur* » La multiplication des incidents de cybersécurité maritime cette année ne peut que lui donner raison.

Le trafic maritime est donc un terrain de choix, vu les enjeux économiques, pour les attaques des pirates, tant informatiques que réels. Bruno Bender, coordonnateur cyber pour le monde maritime du Comité France Maritime, est revenu sur les principaux incidents de cybersécurité maritime en 2020 et leurs modes opératoires. Ont été ainsi recensées en 2020 plus de 9 attaques cyber d'ampleur sur le

trafic maritime, que ce soit du spoofing de l'AIS (janvier 2020, Ile d'Elbe, Mer de Chine, en Californie en mai, le centre Otan de la méditerranée en 2020…) une attaque ISR en avril 2020 dans le Détroit d'Ormuz dans le port de Bandar Abbas, une attaque en mars 2020 contre le port de Marseille – Fos, contre le Suisse MSC en mars 2020 (Source : International Maritime Organization). La plus importante et la plus significative étant l'attaque de grande ampleur qui a eu lieu en septembre 2020 contre l'armateur français CMA - CGM.

Nous sommes en fait passés d'une situation où nous pensions que les cyberattaques ne concernaient pas les navires, puisqu'ils étaient faits pour être en mer, coupés du lien terrestre, que l'impact économique pour les armateurs ou assureurs était considéré comme négligeable et que seuls les navires militaires méritaient que l'on s'occupe de leur sort mais dans une dimension d'agression ou de réponse dans un environnement de cyberguerre haut du spectre et centrée sur des points névralgiques, à la constatation que la menace cyber concerne l'ensemble des acteurs du maritime, « de la terre à la mer, du civil au militaire » pour reprendre la formule du CyberCercle.

De ce point de vue, un chantier naval, qui figure ainsi parmi les activités industrielles les plus complexes à gérer, doit faire face, à travers la numérisation accrue de ses acteurs, et l'engagement résolu vers l'industrie du futur, aux enjeux de la cybersécurité.

Des enjeux de sécurité qui dépassent le champ strict des acteurs maritimes

La cybersécurité maritime concerne non seulement tous les acteurs maritimes et portuaires (militaires, marine de commerce, transport de passagers, marine de pêche, plaisance, métiers portuaires, assureurs) mais aussi, via ses flux commerciaux et les répercussions économiques sur l'hinterland, le commerce et l'économie mondiale dans son ensemble. Le développement des ports, des escales plus courtes, l'automatisation des bâtiments et le développement des systèmes embarqués, voire même le projet de de « navire connecté autonome » lancé en septembre dernier avec IBM (source : https://www.journalmarinemarchande.eu/filinfo/le-navire-autonome-lance-le-16-septembre), légitiment toutes les interrogations et une préoccupation majeure sur ce secteur.

Pour Jean-Marie DUMON, délégué général adjoint du GICAN, la question de la cybersécurité maritime renvoie ainsi à la *notion de « territoire de confiance ».* Pourquoi « territoire de confiance » ? Parce que *cette notion de territoire élargit le concept, lui restitue sa dynamique, sa logique de flux, d'espaces successifs et hétérogènes* et oblige à réfléchir depuis le large dans ses trois dimensions jusqu'à l'Hinterland le plus éloigné. Le projet de smart port city du Havre s'inscrit ainsi dans une *approche globale du « smart and secure ».*

Au-delà, la cybersécurité maritime, par l'importance du littoral français et son rôle d'entrée dans l'espace maritime européen (Manche, Mer du Nord, Atlantique et Méditerranée) se situe bien au-delà d'un enjeu national. Il est européen, voire mondial. Andreas SCHWAB, député européen, l'a ainsi rappelé avec beaucoup de conviction dans la matinée. L'importance de l'attaque sur CMA CGM de septembre 2020 a renforcé début octobre 2020 la réflexion de l'OMI (Organisation Maritime Internationale) https://www.journalmarinemarchande.eu/actualite/shipping/peril-informatique-apres-cma-cgm-lomi, et mobilise tous les acteurs et les instances européennes, dont l'ENISA.

Une démarche française pro-active et une nécessaire coopération internationale

L'ensemble des acteurs de maritime se sont engagés dans une réflexion de fond pour répondre à ces enjeux de cybersécurité, que ce soit au niveau national, européen ou international.

Jean-Marie DUMON et Bruno BENDER ont donné la mesure de l'ampleur du sujet. Brest, officiellement choisie le 17 novembre 2020 pour être le siège du CERT Maritime et qui entend à devenir un pôle d'excellence sur le sujet, via la création de France Cyber Maritime, prendra une part active de coordination de la réflexion nationale. La densité du trafic maritime sur le rail d'Ouessant, porte d'entrée en Manche vers la Grande Bretagne et les ports de la Manche et de la Mer du Nord (Le Havre, Dunkerque, Anvers, Rotterdam, Bremerhaven, et, via la Mer Baltique, les ports polonais, baltes et

russes) légitime la place de Brest sur ce sujet, mais d'autres organisations se sont mises en place en France, comme le CRC2 de la région SUD.

De manière plus opérationnelle la Gendarmerie Maritime a établi un dispositif de lutte contre les attaques cyber maritime. Le commandement est situé à Houilles, avec trois grands relais à Brest, Cherbourg et Toulon. L'intervention de Stéphane FRONCZAK, chef de la cellule CYBERGENDMAR, a établi l'ampleur de la tâche : « Pirater ou leurrer les systèmes de navigation embarqués comme un IAS ou un GNSS, mener des opérations de phishings et de ransomwares, deviennent des vecteurs d'attaque récurrents. Les assureurs spécifiques du secteur maritime commencent à entamer une réflexion de fond sur le sujet, tant l'enjeu est majeur. »

Au niveau européen, l'ENISA s'est saisi de ce sujet depuis quelques années. Ainsi le nouveau document de l'ENISA sur les ports, Cyber risk management for ports, est paru en décembre 2020 : https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

Au niveau international, les exigences de l'OMI en matière d'intégration du cyberisque dans les systèmes de gestion de la sécurité à bord, via la résolution MSC.428 (98) adoptée en 2017, sont entrées en vigueur le 1er janvier 2021 pour les armateurs et les compagnies maritimes https://marine-offshore.bureauveritas.com/magazine/imo-2021-puts-spotlight-cyber-security

La réflexion sur la cybersécurité maritime est donc aujourd'hui nationale, européenne et internationale, l'actualité récente accélérant d'autant les actions entreprises. Depuis l'Antiquité, le trafic maritime contribue au développement du commerce mondial. Sa sécurité n'est pas en soi une nouveauté, mais l'importance de la surface d'attaque cyber qu'offre le trafic maritime aujourd'hui est un enjeu majeur de sécurité et de développement au niveau mondial.

***

Le port du Havre, pionnier dans l'approche cyber

HAROPA - Port du Havre, une réflexion de cybersécurité intégrée à la gestion des risques portuaires

De par son importance dans le commerce français et européen, le Port du Havre qui compte plus de 600 entreprises et pas loin de 22 000 salariés, s'est positionné depuis plusieurs années comme un acteur pionnier dans le domaine de la cybersécurité. L'objectif de cette réflexion novatrice est de faire de la cybersécurité un élément différenciant de l'ensemble HAROPA- Port du Havre vis à vis de la concurrence internationale intense que se livrent les ports de la Manche et de la mer du Nord, tout en devenant un acteur fédérateur de la réflexion en France dans ce domaine.

Baptiste MORAND a rappelé dans son discours d'introduction l'importance de l'axe seine la Vallée de la Seine (axe le Havre / Rouen) en lien avec le Bassin Parisien, « *qui se concrétisera, par la fusion des ports du Havre, de Rouen et de Paris au 1er juin 2021 ».*

Le Port du Havre a donc, depuis plusieurs années, intégré la cybersécurité, non seulement des infrastructures, mais de toute l'activité économique au trafic maritime, dans une vision stratégique de l'activité d'un port. Cette vision cyber s'articule autour de deux axes dont s'est félicité Baptiste MORAND : le premier axe, par un partenariat stratégique établi entre HAROPA - Port du Havre et l'ANSSI, qui se concrétise notamment par des tests grandeur nature, et le deuxième, par une vision territoriale autour d'un écosystème du port et de son environnement immédiat (atterrissage des bâtiments, arrivée dans le port, lamanage, déchargement/ chargement), mais aussi la chaine logistique et l'approvisionnement du pays , voire de l'espace européen et international (l'hinterland).

Jérôme BESANCENOT, chef du service du développement des systèmes d'information d'HAROPA - Port du Havre, a détaillé dans la journée des RCyberNormandie, le projet CYMPATI (Cybersécurité Maritime, Portuaire et industrielle), une plateforme de cybersécurité maritime, portuaire et industrielle. Ce projet, couplé au Havre Smart Port City, qui intègre le cadre de l'action locale, coordonne l'action des industriels portuaires, de l'UMEP, de l'enseignement et de la recherche, de SOGET et d'autres partenariats industriels. Il vise non seulement à fédérer les acteurs de la vallée de la Seine, mais aussi à sécuriser l'ensemble de l'écosystème portuaire exposé aux cyberattaques. Ce projet inclut non seulement une tactique et une réflexion au long cours sur une culture de management du Cyber Risk spécifique au secteur portuaire, mais aussi le projet d'un SOC Portuaire interfacé avec le centre de Coordination Cyber Maritime, et l'Isaac Maritime Européen. Un projet innovant et d'une grande ampleur à suivre.

Merci à Sylvaine LUCKS de sa contribution pour cet article.