CYBER CERCLE
collection

CYBERSÉCURITÉ MARITIME

Regards croisés

Christophe AUBERGER
Juliette AVIGNON
Laurent BANITZ
Bruno BENDER
Jérôme BESANCENOT
Jean-Marie DUMON
Stéphane FRONCZAK
Olivier JACQ
William LECAT
Olivier LASMOLES
Florian MANET
Frédéric MONCANY de SAINT-AIGNAN
Jérôme NOTIN

Préface de Bénédicte PILLIET

2020

Préface

BÉNÉDICTE PILLIET
Présidente, CyberCercle

En décembre 2013 le Livre Bleu de la Marétique mettait en exergue la notion de systèmes de transport intelligents. A plusieurs reprises, les termes «interopérabilité», «nouvelles technologies numériques», «nouveaux usages» ou «compétitivité», des projets comme le «*On board assistant*» ou le «système intégré de navigation» étaient abordés. Mais rien ou à peine sur la cybersécurité, évoquée succinctement à la page 15 en termes de «bulle sécurité» et en omettant les systèmes industriels.

Ce constat a été à l'origine dès 2014 de la démarche du CyberCercle sur la cybersécurité maritime, à la demande de l'amiral Coustillière, alors officiel général cyberdéfense au ministère de la Défense. En 2015 nous créions les Rencontres Parlementaires Cybersécurité & Milieu Maritime, événement annuel, avec un objectif : participer au développement d'une culture de cybersécurité au sein des acteurs du monde maritime « *de la terre à la haute mer, du civil au militaire* », en favorisant le partage de connaissances entre spécialistes de la cybersécurité, parlementaires et acteurs du maritime.

Une démarche innovante alors en France dans le secteur maritime.

Depuis 2015, la cybersécurité maritime constitue ainsi un axe majeur de l'action du CyberCercle, à travers cette journée annuelle de Rencontres, mais aussi des petits-déjeuners-débats dédiés, des lettres d'information et un travail de fond avec les parlementaires.

Force est de constater que, si les progrès ont été rapides en matière de cybersécurité maritime militaire, notamment sous l'impulsion du ministre de la Défense Jean-Yves Le Drian, le monde civil de la mer a mis plus de

temps à prendre en compte cette dimension dans ses actions collectives, alors même qu'il faisait l'objet d'attaques qui se sont accentuées ces dernières années. Les grandes compagnies maritimes MAERKS, COSCO, MSC, CMA-CGM, ainsi que les ports de San Diego, de Barcelone ou de Bandar Abbas, et même l'Organisation Maritime Internationale… autant d'acteurs qui ont eu à subir des cyberattaques majeures, sans compter celles sur lesquelles il n'y a pas eu de communication.

2019 a enfin vu la définition sous l'égide du Secrétaire Général de la Mer d'une feuille de route interministérielle pour la cybersécurité maritime. Dans son prolongement, l'association France Cyber Maritime vient de voir le jour en décembre 2020 à Brest et un projet de M-CERT est en cours de création. Le C2RC, Centre de Ressources Régional Cyber de la Région SUD, inauguré en octobre 2020 à Toulon, a également inscrit la cybersécurité maritime dans sa feuille de route.

Nous ne pouvons que nous réjouir au CyberCercle de cette montée en puissance et de ce début d'actions opérationnelles collectives portées par les acteurs même du maritime.

Mais la route est encore longue, nous le savons tous.

C'est ainsi pour faire le point sur les enjeux, les actions déjà conduites mais également celles qui devront demain être menées, que nous avons consacré le premier opus de notre nouvelle collection d'ouvrages collectifs du CyberCercle au traitement de cette thématique.

Non pas comme un aboutissement de notre travail depuis 2014, mais comme un point de départ de ce que tous nous aurons à conduire.

Le CyberCercle continuera pour sa part à travailler sur ces questions, non seulement à travers son rendez-vous annuel, mais aussi avec le CyberCercle Maritime qui, tous les deux mois, traitera de ce champ dans ses matinales, sous la présidence des élus et dans l'esprit fédérateur qui est le nôtre.

Je tiens à remercier l'ensemble des contributeurs d'avoir accepté de partager leur expertise et leur vision de cette thématique majeure, ainsi

que nos partenaires, Cybermalveillance.gouv.fr, le GICAN, FORTINET et CERTitude NUMERIQUE qui ont contribué avec nous au financement de cet ouvrage.

Donner des clefs de compréhension aux décideurs et à tous ceux qui aiment la Mer pour faire de la France Maritime de demain une référence internationale en matière de sécurité numérique, un acteur majeur de confiance pour le commerce maritime, un interlocuteur fiable pour la défense navale, et un facteur de développement pour les territoires : tel est l'objet de cet ouvrage.

« *Seul on va plus vite, ensemble on va plus loin* » : cette maxime que le CyberCercle a fait sienne depuis sa création est encore plus vraie pour les acteurs du maritime.

Je vous souhaite une bonne lecture.

Cybersécurité maritime, un enjeu stratégique pour tous les acteurs de la filière

CHRISTOPHE AUBERGER
Directeur technique, évangéliste Cybersécurité, FORTINET

La première cyber arme, STUXNET, découverte en juin 2010 a détruit partiellement le programme nucléaire Iranien, c'était d'ailleurs son objectif. Cela a très probablement déclenché des représailles conduisant à l'arrêt de l'ensemble des réseaux de Saudi Amamco en 2012. Il s'agissait des premières salves d'une nouvelle forme de guerre avec laquelle nous devons vivre maintenant. La course a`ce type d'armes a fait prendre conscience de la réalité des menaces cyber qu'elles concernent, comme l'exfiltration de données, le sabotage, le terrorisme, le piratage ou l'espionnage.

Il n'y a aucune raison objective pour que certains secteurs de l'activité humaine soient épargnés, à plus forte raison si ces secteurs sont fortement numérisés. Il serait faux de penser que le navire est un moyen de transport a`l'écart de ces risques. La numérisation touche tous les secteurs y compris le monde maritime et ce dernier entre, comme beaucoup d'autres, dans le monde de l'hyperconnexion : liste des cargaisons précieuses, traçage et acheminement intelligent, objets connectés, ravitaillement prédictif, positionnement assisté des charges, optimisations portuaires... Ainsi l'écosystème, navire, cargaisons et infrastructures portuaires, deviennent des cibles pour les cybercriminels.

Évidemment, comme dans de nombreux autres domaines, les risques ne sont pas toujours les mêmes en fonction du type de navire et de son activité. On comprend intuitivement que la localisation d'un navire n'a pas le même impact selon qu'il s'agisse d'un navire militaire en mission, d'un porte-conteneurs en transit ou d'un yacht de plaisance. Les risques, le ciblage et les impacts sont différents selon que l'on s'intéresse à la marine

marchande, militaire, les compagnies de croisière ou la navigation de plaisance. Pour autant ces risques sont réels et déjà plusieurs attaques ont été recensées dans ce domaine.

En 2016, Verizon indiquait dans son rapport d'analyse des incidents avoir identifié une menace visant une compagnie maritime. Les cybercriminels s'étant introduits dans le système d'information de l'entreprise avaient accès aux listes de marchandises précieuses transportées a`bord des navires. Ils pouvaient ensuite récupérer les marchandises en envoyant des équipes sur place. Il s'agissait de vols ciblés en quelque sorte. Dans ce cas d'une cible du monde maritime, l'attaque en elle-même visait un système d'information classique mais aussi des applications spécifiques et vulnérables.

Si nous regardons d'un peu plus près quelles sont les vulnérabilités potentielles des navires, nous constatons que les attaques peuvent être liées à :

- la cybercriminalité classique dont la motivation est financière, il s'agit de loin de la partie la plus importante, au moins en volume;
- l'intelligence économique offensive (atteinte a`l'image de la compagnie du navire);
- des actions tactiques ou stratégiques d'états à l'encontre de bâtiments militaires ;
- le cyber-espionnage commercial;
- le cyber-sabotage.

Aujourd'hui, même si les exemples d'attaques visant un navire restent relativement limités, il y a peu de doute quant à leur augmentation à l'avenir et il convient de prendre ce risque en charge. Les exemples touchant l'industrie maritime se multiplient d'ailleurs: port d'Anvers, douanes australiennes, malwares Zombie Zero ou Icefog ciblant les acteurs maritimes ou encore Maersk en juin 2017 via Notpetya ayant causé une perte d'exploitation de près de 300 millions de dollars. L'objectif de cyberdéfense des navires est de garantir que la conduite et l'exploitation ne pourront être affectées par une cyberattaque. L'Organisation maritime internationale (OMI ou IMO en anglais) qui est l'institution spécialisée des Nations Unies chargée d'assurer la sécurité et la sûreté des transports

maritimes a d'ailleurs édité les lignes directrices relatives à la cybersécurité des navires sous forme d'une circulaire de juillet 2017 (MSC-FAL.1/Circ.3). Il y a aussi le règlement européen CE725/2004 article 3.5 qui rend obligatoire pour tout pavillon français une évaluation de la sécurité des systèmes d'information du navire.

Le monde maritime est en pleine mutation, la transformation numérique est en cours et nous pouvons notamment citer la méthodologie STM (Sea Traffic Management, gestion du trafic maritime) développée par l'administration maritime suédoise, et plus particulièrement le projet MonaLisa, approuvé par la Commission européenne et qui est maintenant en version 2.0. Ce projet cherche à définir un ensemble de systèmes et de procédures pour guider et surveiller le trafic maritime d'une manière similaire à la gestion du trafic aérien. La version 2.0 intègre la dimension cybersécurité et les procédures de connexion et chiffrement que le navire soit en route via satellite ou à quai via WiFi, 4/5G, ou filaire.
L'objectif est de fournir à toutes les parties intéressées et autorisées de la chaîne de transport, des informations en temps réel afin d'améliorer la sécurité, la sûreté et l'efficacité. C'est une approche similaire au système SENIN de la marine nationale mais à visée civile. L'objectif est également l'élévation du niveau de cybersécurité des navires en appliquant un ensemble de règles qui intègrent la gestion des systèmes industriels du navire, la gestion des outils technologiques, la formation du personnel et des procédures intégrées au niveau des codes déjà établis par l'OMI.

Afin de couvrir les risques et d'assurer une cyber-résilience importante des navires, il convient de définir si ces environnements comprennent des spécificités et lesquelles. Les cyber-risques potentiels pour un navire sont de plusieurs ordres du fait des différents sous-ensembles qui composent son système d'information :

- un navire c'est d'abord un ensemble de systèmes industriels embarqués, un réseau opérationnel (ICS) qui se déplace avec tous les risques et contraintes spécifiques;
- un navire c'est aussi un flot de données très important traité par un système informatique classique de plus ou moins grande envergure selon le contexte, sur les bâtiments de croisière, véritables villes flottantes, ils sont extrêmement étendus et complexes et comprennent des réseaux

publics (notamment pour préserver le moral des équipages en leur permettant de communiquer avec leur proches, ou de proposer un accès Internet aux passagers);
- un navire c'est enfin un ensemble de systèmes opérationnels spécifiques utilisés pour l'identification, la navigation, le positionnement (AIS, RADAR, GNSS, VDR, ECDIS…) voire des systèmes d'armes dans le cas de navire militaires.

Les systèmes industriels embarqués

Les technologies opérationnelles, les outils de traitement automatisés des environnements industriels sont encore aux premiers stades d'appréhension des problématiques de cybersécurité mais doivent avancer rapidement dans ce domaine afin de faire face à la convergence numérique qui se produit dans ce secteur. Ce domaine dans les navires ou les infrastructures portuaires ne déroge pas à ce constat. La vulnérabilité´des systèmes industriels est connue et les attaques ciblées ont démontré leur efficacité en termes de vol de données, d'intrusion ou de sabotage. Les failles du système industriel sont liées aux constats suivants :
- l'absence de cloisonnement entre les systèmes d'information générale et les systèmes industriels non sécurisés;
- le faible niveau de protection des accès avec des contrôles parfois inexistants ou très simples, l'usage généralisé de compte administrateur et l'absence de protection sur les terminaux d'accès;
- le très faible niveau de mise à jour et l'utilisation de protocoles non fiables et non chiffrés (FTP, Telnet, VNC, SNMP...) ;
- le manque de vision et d'intégration de la sécurité dans les développements souvent internes;
- le manque de surveillance des anomalies;
- l'intégration toujours croissante de système non durcis disponibles facilement (PC, Rasberry, cartes Intel...) et non maitrisés voire non connus des équipes en charge (shadow IT)
- le non contrôle des intervenants sur les systèmes comme les sous-traitants ou les mainteneurs.

Il conviendra donc de ne considérer aucune zone comme étant de confiance et de mettre à minima en place des solutions de segmentation, voire de micro-segmentation.

Les données navales

L'arrivée des nouvelles technologies ou plus généralement la transformation numérique du secteur entraîne une évolution critique du volume et de l'importance des données traitées pour et par le navire. En raison de la croissance exponentielle des données numériques, le besoin de gestion et de sécurité de celles-ci devient le premier enjeu des activités maritimes. Les masses de données hétérogènes sont une importante source d'amélioration et d'optimisation des activités et leur exploitation pertinente constitue une aide précieuse à la prise de décisions. Mais elles constituent aussi, compte tenu du domaine sensible et des conséquences en cas de manipulation ou exploitation malveillante de ces informations, un risque majeur. Il s'agit d'un enjeu stratégique, y compris en ce qui concerne les navires commerciaux de transport de marchandises ou de passagers. D'autant que le secteur fait de plus en plus appel aux objets connectés ou aux systèmes embarqués insuffisamment protégés. La gestion des données au sens large est donc au centre des activités maritimes et de la défense navale. Cela nécessite la mise en place d'une vraie politique de sécurité des données, intégrant la détection des tentatives d'intrusion, des codes malveillants, des fuites de données et des comportements suspects.

Les systèmes opérationnels spécifiques

En tant qu'unité mobile, un navire dispose de nombreux équipements spécifiques permettant d'assurer sa conduite opérationnelle. Ces équipements sont encore plus nombreux et sensibles sur les navires militaires avec les différents systèmes d'armes, les outils d'échange d'information tactiques, les équipements de guerre électronique… Aujourd'hui nombreux sont ces équipements qui sont interconnectés avec le réseaux internes industriels et par conséquent avec l'ensemble des systèmes de traitement de l'information multipliant ainsi les risques d'attaques spécifiques. Un des systèmes les plus importants aujourd'hui est celui permettant de se positionner avec précision : le système satellite de navigation mondiale (GNSS). L'un des problèmes inhérents à cette technologie est que les signaux des satellites civils ne sont pas protégés par chiffrement. Il est donc possible de les intercepter et de les dupliquer, cela

induit des vulnérabilités particulières comme la possibilités d'interférence volontaire ou non ou encore la possibilité de brouillage intentionnel. De nombreux systèmes spécifiques des navires intègrent également un ordinateur et un ensemble de logiciels plus ou moins importants qui permettent d'assurer des fonctions opérationnelles ou l'interface avec les exploitants. C'est le cas du VDR (enregistreur de voyage), du système d'affichage électronique des cartes (ECDIS), l'aide au traçage radar automatique (ARPA) ou encore le système d'identification automatique (AIS). Tous ces systèmes intègrent un système provenant d'un industriel du secteur généralement non durci et fonctionnant sous un système d'exploitation (très souvent Microsoft Windows) standard du marché. Il est donc impératif que ces systèmes soient maintenus à jour et que les mises à jour de sécurité soient systématiquement déployées.
A titre d'exemple l'AIS, base´sur l'échange automatique d'information entre navires entre eux et centres de surveillance maritime, permet une identification en temps réel des navires émetteurs, il est de par sa conception, vulnérable au brouillage et aux virus informatiques. Une fois infecté, le système pourrait diffuser de fausses informations comme un signal de détresse, ou une fausse localisation de navire afin de piéger le navire victime.

Quelle approche pour la cyberdéfense des navires ?

Bien que l'environnement maritime soit spécifique sur certains aspects, la cybersécurité et les approches associées ne différent pas d'autres environnements. Tout au plus, il pourrait être nécessaire dans certains cas de disposer de technologies dont les équipements supportent certaines normes comme IEC 61162-460, IEC 60945 ou être résistants aux menaces TEMPEST. Aujourd'hui cela peut être facilement réalisé en implémentant les technologies sous forme de machines virtuelles au sein de matériel déjà homologué pour ces normes. Ainsi nous avons des exemples de plus en plus nombreux de déploiements de solutions permettant de couvrir certains risques maritimes. Nous pouvons citer par exemple le déploiement d'accès wireless passagers sécurisés pour la flotte de navires de croisières de Marella Cruise. Dans un contexte plus large, NexusOcean a déployé au sein de sa flotte à la fois les fonctions de réseau intelligent sécurisé (y compris des fonctions de SD-Wan) pour protéger

et optimiser l'utilisation des liens de connexion (VSAT). NexusOcean a déployé également des fonctions de segmentation et de micro-segmentation afin d'isoler les différents sous-ensembles des navires, y compris les réseaux industriels opérationnels pour défendre l'ensemble de l'infrastructure contre les cybermenaces. Il y a également d'autres compagnies de croisières qui ont déployé des solutions de contrôle d'accès et de profilage des objets connectés (zero trust network access) afin de s'assurer que les équipements qui communiquent avec l'infrastructure du navire sont bien ceux qu'ils prétendent être et ont bien le droit d'accéder aux ressources qu'ils demandent.

Nous n'en sommes qu'au début, les progrès technologiques dans le secteur du transport maritime, comme les navires autonomes, les drones et diverses applications utilisant les blockchains, sont particulièrement prometteurs pour l'offre de transport maritime mais les acteurs du secteur restent incertains notamment quant aux risques de cybersécurité. Le secteur doit clairement rattraper son retard et un effort important d'évangélisation et de sensibilisation est impératif.

Cyber-combattant et Marin : quand la Marine Nationale ouvre le champ des possibles

Capitaine de Frégate JULIETTE AVIGNON
Adjoint à l'autorité du domaine de compétences SIC, Bureau du Numérique,
Etat-major de la Marine Nationale

La Marine nationale opère dans tous les milieux : en surface avec la force d'action navale, sous la mer avec la force océanique stratégique, dans les airs avec l'aéronautique navale et sur terre avec les actions terrestres menées par les fusiliers marins et commandos. Le cyberespace est désormais reconnu comme un nouveau milieu présentant de remarquables opportunités mais aussi de redoutables menaces et s'impose comme un espace de conflictualité. La Marine nationale se doit d'y être présente.

Fidèle aux amers stratégiques définis par son chef d'état-major dans le plan Mercator, la Marine ouvre une nouvelle voie dans ses opérations aéronavales afin de rester « une marine de combat, en pointe et qui compte sur chacun ».

Cyberdéfense, cyber-protection ou cyber-offensive sont des thématiques en devenir dont la dynamique dans les années à venir n'est plus à démontrer. Le domaine étant fortement concurrentiel, la Marine entend bien remporter la bataille du recrutement, de l'attractivité et des compétences en offrant de belles opportunités de formation, de progression et des perspectives de carrières variées. Ainsi, il est désormais possible d'être marin et cyber combattant.

Le Cyber : un domaine en devenir

Une Marine en pointe

La numérisation des unités de combat offre des capacités et des perspectives opérationnelles tant dans le domaine des communications que du renseignement, du combat collaboratif mais aussi du soutien des

forces et de la maintenance. Véritables systèmes d'information flottants, les bâtiments de la Marine nationale multiplient les capteurs déportés sous forme de drones, aériens ou sous-marins, lui permettant de voir au-delà de l'horizon et ainsi de mieux maîtriser son environnement. Ces plateformes inhabitées placent le navire au cœur d'un réseau local d'échange de données en pleine mer. Le centre des opérations devient alors un nœud d'objets connectés, formidables atouts opérationnels mais également sources de vulnérabilités qu'il convient de protéger. Leur maîtrise, leur sécurité et leur résilience sont déterminantes pour assurer la réussite de la mission.

Entrée de plain-pied dans l'ère du numérique, avec la récente mise à niveau Cyber des frégates multi-mission (FREMM), la problématique Cyber est désormais intégrée aux grands programmes d'armement dès leur conception. C'est notamment le cas pour les frégates de défense et d'intervention (FDI), les sous-marins nucléaire d'attaque (SNA) de type *Suffren*, mais aussi pour le futur porte-avions de nouvelle génération, successeur désigné du *Charles de Gaulle*. Ces bâtiments disposeront d'un SOC[1] embarqué connecté au SOC Marine. Des réflexions sont également menées sur la constitution et l'utilisation de Clouds privés ou dédiés, de métropole ou de théâtre et font naître de nouveaux besoins pour de nouveaux métiers, notamment dans les domaines du Big Data ou de l'intelligence artificielle.

… qui nécessite des compétences et des formations spécifiques

Lutte informatique défensive (LID), maintien en condition de sécurité (MCS) ou encore sécurité des systèmes d'information (SSI) sont autant de domaines pour lesquels la Marine recrute et forme.

La Marine doit assurer la sécurité de ses 600 systèmes d'informations (SI) métiers dans le domaine des opérations, des RH, de la maintenance mais aussi celle de ses multiples réseaux qui peuvent être classifiés ou non, internes, externes, interarmées ou interalliés, déployés en métropole, en mer ou à l'étranger. Afin de garantir son autonomie opérationnelle et stratégique, ces fonctions essentielles ne peuvent être sous-traitées. Ainsi, la Marine emploie des techniciens et spécialistes de tous niveaux, tels que des administrateurs en cybersécurité, des analystes cyberdéfenses ou encore des auditeurs en SSI.

Le choix d'une génération de compétences en interne, via un partenariat avec l'Ecole des Transmissions (ETRS) de l'armée de Terre pour les techniciens de la Marine puis la création d'une formation Cyber au Pôle Ecoles Méditerranée (PEM) à Saint-Mandrier pour passer au niveau supérieur s'est naturellement imposé comme la solution la plus à-même de garantir l'adéquation entre la formation et les besoins opérationnels. En outre, elle permet aux marins de progresser dans l'institution tant sur le plan technique que managérial.

En sus des formations de cursus déjà mentionnées, des stages et des formations en continu sont proposées tout au long de la carrière du marin, quel que soit son niveau, pour adapter ses compétences à l'exercice de son métier. Un catalogue de stages de qualité, dispensés par l'ANSSI ou les centres de formations de la Défense, permet au marin d'actualiser ses connaissances et d'être toujours à bon niveau, et au fait (« *up-to-date* ») des évolutions technologiques.

Par ailleurs, une chaire de Cyberdéfense des Systèmes Navals a vu le jour en 2014 à l'Ecole Navale, l'école des officiers de Marine, en partenariat avec Naval Group, Thalès et IMT Atlantique, et un Mastère spécialisé en cybersécurité des systèmes maritimes et portuaires ouvrira ses portes en septembre 2020 plaçant ainsi la Marine nationale au cœur du pôle d'excellence cyber et lui octroyant un rayonnement à portée nationale et internationale dans le domaine de la recherche.

Une dynamique RH qui ne se dément pas !

Une priorité du ministère des Armées

Le Cyberespace en général et la cyberdéfense en particulier, ont été identifiés dans la Loi de programmation militaire (LPM) comme une priorité ministérielle. Pour y répondre positivement, la Marine souhaite renforcer ses capacités en LID, SSI et MCS mais aussi voir l'apport de la lutte informatique offensive (LIO) et de la lutte informatique d'influence (LII) croître au profit des opérations dans le milieu aéro-maritime. L'avènement de la transformation digitale, de data centers embarqués ou à terre et l'émergence de l'intelligence artificielle participent à la croissance fulgurante des besoins en ressources Cyber pour la Marine. Ce besoin est

particulièrement prégnant dans la mise en œuvre de la cyberdéfense embarquée.

Aujourd'hui, ce sont près de 270 postes identifiés Cyber qui sont occupés par des marins dans et hors de la Marine dont 58% pour les officiers mariniers et 42% pour les officiers. D'ici 2025, la LPM prévoit pour la Marine ? une montée en puissance de 56 officiers mariniers et 49 officiers dans ce domaine.

Des recrutements à tous les niveaux
Conforme au modèle « d'escalier social » qu'elle promeut, il est possible d'entrer dans les rangs de la Marine sans diplôme et d'y acquérir les compétences nécessaires pour progresser dans l'institution, y compris dans des métiers aussi en pointe que ceux de la Cyber.

Un jeune, à partir de 17 ans, de niveau 3ème à Bac peut s'engager comme matelot de la Flotte et intégrer des fonctions d'opérateur élémentaire de systèmes d'informations et de communication avant de suivre le cours du brevet d'aptitude technique (BAT) dans la spécialité SITEL – système d'information et de télécommunication – à l'école de Maistrance. Cette filière, actuellement en cours de réforme, permet notamment d'acquérir les bases des connaissances en cyberdéfense et ouvre la voie vers des métiers de techniciens orientés SI, Réseaux ou Télécommunication. Au fil des Une dynamique RH qui ne se dément pas !

Une priorité du ministère des Armées
Le Cyberespace en général et la cyberdéfense en particulier, ont été identifiés dans la Loi de programmation militaire (LPM) comme une priorité ministérielle. Pour y répondre positivement, la Marine souhaite renforcer ses capacités en LID, SSI et MCS mais aussi voir l'apport de la lutte informatique offensive (LIO) et de la lutte informatique d'influence (LII) croître au profit des opérations dans le milieu aéro-maritime. L'avènement de la transformation digitale, de data centers embarqués ou à terre et l'émergence de l'intelligence artificielle participent à la croissance fulgurante des besoins en ressources Cyber pour la Marine. Ce besoin est particulièrement prégnant dans la mise en œuvre de la cyberdéfense embarquée.

Aujourd'hui, ce sont près de 270 postes identifiés Cyber qui sont occupés par des marins dans et hors de la Marine dont 58% pour les officiers mariniers et 42% pour les officiers. D'ici 2025, la LPM prévoit pour la Marine ? une montée en puissance de 56 officiers mariniers et 49 officiers dans ce domaine.

Des recrutements à tous les niveaux
Conforme au modèle « d'escalier social » qu'elle promeut, il est possible d'entrer dans les rangs de la Marine sans diplôme et d'y acquérir les compétences nécessaires pour progresser dans l'institution, y compris dans des métiers aussi en pointe que ceux de la Cyber.

Un jeune, à partir de 17 ans, de niveau 3ème à Bac peut s'engager comme matelot de la Flotte et intégrer des fonctions d'opérateur élémentaire de systèmes d'informations et de communication avant de suivre le cours du brevet d'aptitude technique (BAT) dans la spécialité SITEL – système d'information et de télécommunication – à l'école de Maistrance. Cette filière, actuellement en cours de réforme, permet notamment d'acquérir les bases des connaissances en cyberdéfense et ouvre la voie vers des métiers de techniciens orientés SI, Réseaux ou Télécommunication. Au fil des affectations, le jeune maistrancier acquiert de l'expérience et peut prétendre à davantage de responsabilités. Une spécialisation Cyber lui est ensuite accessible, au niveau brevet supérieur (BS), en suivant les cours dispensés par l'armée de Terre à l'ETRS.

En fonction de son niveau scolaire, un jeune peut intégrer cette filière à différents niveaux : un titulaire du Bac peut s'engager dès le BAT et un titulaire d'un BTS ou Bac+2 peut passer par la toute récente filière des BS-ab Initio qui permet au jeune d'obtenir son BS en moins de 2 ans et de capitaliser ainsi sur des connaissances académiques acquises dans le circuit de l'éducation nationale.

Enfin, la Marine recrute également des officiers Bac+3 et plus, notamment des officiers sous contrats spécialisés dans la Cyberdéfense pour occuper des postes d'experts.

Cyber-combattant et Marin : 2 passions pour 1 métier

Des métiers valorisants
Les métiers cyber permettent au marin d'opérer des systèmes complexes et évolutifs.

Chargés du maintien de la sécurité des services des réseaux et des données qui y transitent, les administrateurs en cybersécurité doivent être en mesure de détecter les intrusions, les codes malveillants et leur éventuelle propagation. Ils mettent en œuvre des solutions de chiffrement et sont également capables de simuler un affrontement dans le cyberespace à des fins d'entraînement de la chaîne de LID.

Les analystes cyberdéfense, outre leurs connaissances réglementaires et juridiques du domaine de la SSI, effectuent des recherches de compromissions en exploitant des sondes gouvernementales ou commerciales. Ils sont également formés à la gestion de crise tant pour la communication vers les personnes et organismes concernés que pour coordonner les actions de résolution entre les différentes parties prenantes.

Les auditeurs SSI identifient quant à eux les vulnérabilités des systèmes d'information et permettent de réaliser leurs homologations et maintien en condition de sécurité.

Pour un officier marinier, le niveau d'expertise le plus élevé du domaine est atteint par l'obtention du brevet de maîtrise Cyber soit par la voie académique, via la formation dispensée au PEM, soit par validation des acquis de l'expérience après un parcours qualifiant. Expert de l'action dans le cyberespace, il devient alors le spécialiste SSI capable d'identifier les risques pesant sur les systèmes en production ou en projet et de conseiller les responsables des systèmes pour organiser la défense en profondeur. Egalement expert en LID, il peut préparer, planifier et conduire des opérations dans le cyberespace et organiser la gestion de crise cybernétique.

Les officiers peuvent s'orienter vers des métiers tels que responsable sécurité des systèmes d'information, de conduite de projet, spécialiste ou ingénieur en cyberdéfense.

Des perspectives d'emploi variées
Certains organismes sont spécifiquement dédiés aux questions relatives à la cyberdéfense. C'est notamment le cas du centre support à la cyberdéfense (CSC) de la Marine. Véritable pôle d'expertise en LID, il agit en soutien des unités de la Marine et organise les missions d'entraînement et les exercices nationaux type DEFNET ou E=MC.

Le centre de renseignement et de guerre électronique (CRGE) dispose d'une cellule spécialisée en renseignement d'intérêt cyber (RIC) d'application militaire, principalement dans le domaine maritime.
Le bureau des systèmes d'information et de communication et du numérique (BNUM) de l'état-major de la Marine est doté d'une section Cyber plus particulièrement chargée de l'homologation des SI Marine.

Néanmoins, le Cyberespace est partout ! La chaîne Cybersécurité irrigue l'ensemble des emprises de la Marine. En particulier, chaque autorité, direction ou service dispose d'un officier cybersécurité positionné au plus près du commandement afin de conseiller et de répondre aux enjeux en terme de SSI, d'homologation et de MCS.

Par ailleurs, la Marine n'est pas le seul employeur de ses marins. Si l'on a déjà vu qu'elle génère en interne ses propres compétences, elle fait bénéficier de son expertise d'autres organismes étatiques. Ainsi, des marins honorent des postes en interarmées voire en interministériel. Il est donc possible d'être affecté à des postes dans des centres interarmées[2], au COMCYBER[3], à la DIRISI[4] ou encore à la DRM[5].

Des Marins avant tout !
La haute technicité des métiers du cyber ne fait pour autant pas oublier que le cyber-combattant est avant tout un marin. Si la progression interne est de mise, c'est que la culture maritime et la connaissance du milieu, des conditions d'usage et de l'environnement des systèmes de forces sont indispensables au bon déroulement des missions des unités de la Marine. Les formations techniques de spécialité s'accompagnent donc de formations maritimes et militaires. Cette culture s'acquiert aussi avec l'expérience développée au sein de l'institution. Ainsi, si la carrière du marin lui permet de cheminer parmi les différents employeurs du

ministère, il est important, pour lui comme pour l'institution, de revenir vers la maison mère et d'alterner autant que possible postes embarqués et postes à terre.

A bord, le cyber-combattant est un membre à part entière de l'équipage du bâtiment de surface ou du sous-marin. Il participe donc à la vie et à la sécurité du bateau, aux exercices de qualification opérationnelle de l'équipage. Comme tout officier ou officier marinier, il est amené à développer tout au long de sa carrière, outre ses compétences techniques, des aptitudes dans le domaine du leadership et du commandement, qualités indissociables des métiers des armes.

Le cyber-combattant de la Marine doit être en mesure de troquer à tout moment sa casquette d'expert, de spécialiste technique, pour celle du marin militaire. Et c'est ce qui fait de lui une ressource si précieuse.

[1] Security Operating Center
[2] Centre d'analyse en LID, Centre d'audit SSI, Centre réserve et préparation opérationnelle de cyberdéfense etc.
[3] Commandement de la cyberdéfense, placé sous l'autorité du chef d'état-major des armées
[4] Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense
[5] Direction du renseignement militaire

Les cyber risques dans le monde maritime : de la prise de conscience aux actes

LAURENT BANITZ

Chargé de mission sûreté et cybersécurité des navires, Sous-direction de la Sécurité et de la transition écologique des navires, Direction des Affaires Maritimes, Ministère de la Transition Ecologique

Dans le monde des transports, comme dans tout domaine où elle constitue une préoccupation majeure, la sécurité est fille de l'accidentologie. Si la sécurité du transport maritime est si hautement réglementée à l'échelle internationale, elle le doit en très grande partie aux leçons tirées des accidents maritimes dont les mers sont le théâtre depuis que les hommes s'y sont engagés.

La convention SOLAS[1], le texte international de référence pour la sécurité de la navigation maritime, en est l'exemple emblématique. Signée le 20 janvier 1914, elle fut le fruit d'une prise de conscience brutale par la communauté internationale maritime de la nécessité de réglementer la sécurité de la navigation après le naufrage du Titanic dans la nuit du 14 au 15 avril 1912.

Les exemples pourraient être multipliés à l'envi, comme celui de la loi américaine de 1990 sur la pollution par les hydrocarbures (Oil pollution act), suivie en 1993 des amendements à la convention MARPOL[2] portant sur l'obligation pour les pétroliers de disposer d'une double coque. Ce furent là les leçons tirées de l'échouage du pétrolier Exxon Valdez en 1989.
Si des écarts et des pratiques douteuses persistent ici et là, la culture de la sécurité est largement adoptée et appliquée par l'immense majorité des acteurs du monde maritime. Pour tout marin, les termes d'échouement, de collision, d'incendie à bord ou d'homme à la mer ont un sens précis et tout à fait concret et les principes de sécurité qui y ont trait ne forment dans l'ensemble pas matière à discussion.

Mais il en va pour l'heure différemment de ce que l'on nomme les cyber

risques. Toujours plus numérisé, plus connecté, le monde maritime est par conséquent toujours plus exposé aux attaques qui peuvent viser ses systèmes d'information essentiels, avec des conséquences potentiellement graves sur la sécurité des personnes, sur le milieu marin et sur l'ensemble d'un pan de l'économie vital aux approvisionnements du pays.

L'émergence il y a une vingtaine d'années de ces risques et leur inquiétante augmentation depuis lors n'ont pas encore suscité la prise de conscience globale que les enjeux qu'ils sous-tendent nécessiteraient. L'attitude circonspecte de certains armateurs devant l'obligation de prise en compte de ces risques dans les systèmes de gestion de la sécurité - introduite par la résolution MSC (428)98 de l'OMI[3] – en témoigne. Les armateurs ne sont d'ailleurs pas seuls à tarder à s'engager résolument dans ce combat. En témoigne la rareté des questions de cybersécurité dans les débats tenus au sein des comités de travail de l'OMI depuis la publication de la résolution citée ci-dessus. On sait certains Etats réticents à l'instauration de mécanismes plus stricts en cette matière.

Pourtant, les signaux d'alerte ne manquent pas. L'attaque subie par le géant danois MAERSK en 2017 ou plus récemment par la compagnie CMA CGM n'en sont que les plus marquants et restent pour l'heure l'arbre qui cache une forêt plus préoccupante encore. Hameçonnages, rançongiciels, vols de données et corruption des systèmes de navigation sont autant de menaces avérées.

Face à ce constat, dont on peut à bon droit s'inquiéter, il convient avant tout de comprendre les ressorts d'une attitude qui n'est certes pas le fait d'une négligence des risques maritimes.

Nous devons d'abord garder à l'esprit que les cyber risques sont un phénomène extrêmement récent, si on le rapporte à la longue histoire de la marine de commerce. Mais c'est peut-être avant tout la nature-même de ce risque qui fait encore obstacle à l'assimilation de la cybersécurité dans la culture de sécurité maritime. On a beau jeu de ressasser l'image du navire moderne comme réseau informatique flottant ou objet connecté sur l'eau, celui-ci reste conduit par des marins et exploité par des armateurs pour qui l'informatique et les réseaux restent des outils extérieurs au cœur de leur

métier. Au risque d'une simplification peut être grossière, on peut penser qu'une des difficultés-clés de la résolution de cette équation est de trouver le point de rencontre entre des informaticiens étrangers au monde maritime et des marins qui ne parlent pas leur langage.

Enfin, il se peut également que la portée et le sens des cyber risques n'aient pas jusqu'ici été expliqués de manière pertinente aux premiers intéressés. On a peut-être trop longtemps communiqué sur cette question en s'appuyant sur des scénarios spectaculaires – prise de contrôle à distance d'un pétrolier, paralysie des systèmes critiques de bord, détournements de navires – là où il eut mieux valu sans doute s'adresser aux marins et à leurs employeurs de manière plus concrète, plus proche de leurs préoccupations d'hommes de l'art. Nul doute que le vol de données commerciales ou les pertes d'exploitation soient des dangers qui parlent plus directement au comité de direction d'une compagnie maritime ou d'un port que les exemples cités précédemment. Or l'implication et la prise de conscience de toutes les parties prenantes constitue la clé de toute politique efficace dans ce domaine comme ailleurs.

Ce tableau serait toutefois tronqué s'il n'était qu'alarmiste. Certes, le choc des consciences n'a pas encore eu lieu mais des frémissements se font sentir et gagnent en amplitude.

La publication le 16 juin 2017 de la résolution MSC (428)98 de l'OMI constitue une étape cruciale dans l'acculturation du transport maritime aux enjeux de cybersécurité. Tout d'abord parce qu'elle clôt le débat entre les partisans d'une assimilation de la cybersécurité à la sûreté – à son adossement au code ISPS[4], donc – et les défenseurs de son intégration dans le cadre plus large de la gestion de la sécurité – via le code ISM[5]. Les armateurs et avec eux les administrations, qui réglementent leur activité, ainsi que les sociétés de classification retrouvent des terres moins inconnues.

Les grands axes d'une politique de sécurité, telle que sous-tendue par la résolution MSC (428)98, sont bien connus. On les trouve décrits presque identiquement dans tous les textes – plans gouvernementaux, comme celui de la loi de programmation militaire française, normes sur la gestion du cyber risque, recommandations et guides de bonnes pratiques destinés aux

opérateurs. Il s'agit toujours de partir d'une analyse du risque, elle-même reposant sur une connaissance détaillée des systèmes à protéger, et d'établir des principes de gouvernance engageant l'entreprise à tous les niveaux. Il s'agit ensuite de déduire des enseignements de l'analyse de risque les règles et les moyens de protection et de défense des éléments critiques (par exemple, les systèmes de navigation et de gestion de la propulsion du navire). Enfin, parce qu'il faut être lucide sur les limites de toute prévention, la cybersécurité est aussi affaire de résilience et de capacité à faire face aux crises.

Le cadre général est désormais posé. Mais le tableau reste encore au stade de l'esquisse. En rattachant la prise en compte de la cybersécurité au code ISM, l'accent a été mis sur la gestion du risque et sa formalisation à travers un système épousant les principes de l'assurance qualité. Aussi l'enjeu réside-t-il désormais dans le contenu concret qui sera donné à ce dispositif formalisé. En d'autres termes, il va bien s'agir pour les compagnies maritimes de mettre en place des règles et des dispositifs efficaces, tant sur le plan technique que sur le plan humain, pour maîtriser les cyber risques.

Comment faire en sorte que cet objectif soit atteint ?

D'abord en fournissant à ceux qui vont devoir mettre en place ces dispositifs les éléments de compréhension et les conseils techniques indispensables. L'initiative prise collectivement par plusieurs groupements d'armateurs sous l'égide du groupement BIMCO[6] de produire des recommandations détaillées sur la mise en œuvre d'une politique de cybersécurité des navires va dans ce sens et est à saluer.

Mais avant toute chose, c'est peut-être dans le dialogue que réside la clé de la réussite collective. Il est illusoire d'espérer que tous les armateurs soient fins prêts pour le rendez-vous du 1er janvier 2021 fixé par l'OMI. Pour les services de l'État qui seront chargés de veiller à la bonne application des objectifs de la Résolution, brandir l'épée de Damoclès de sanctions en cas de non-conformités n'aurait guère de portée pratique.

Aussi la Direction des affaires maritimes française, dans la continuité des actions qu'elle a entreprises avec l'aide de ses partenaires (ANSSI et Marine nationale en particulier) depuis plusieurs années – qui en ont fait une

administration précurseur en la matière parmi ses homologues européens – a-t-elle décidé de s'inscrire dans une démarche d'accompagnement vis-à-vis des compagnies maritimes. Par la diffusion de recommandations techniques d'abord, assorties d'explications sur le sens et la méthode des contrôles qui seront effectués aux sièges des compagnies et à bord des navires. Par des rencontres régulières avec les armateurs ensuite. Parce que le dispositif qui s'instaure à partir de l'année 2021 pose également des défis aux services de l'État et notamment aux services déconcentrés chargés de veiller à la bonne application des normes internationales par le pavillon français.

Ce défi est le symétrique de celui évoqué plus haut, celui de la nécessaire acculturation des « marins » aux enjeux de cybersécurité pour leur métier. Une même question est désormais posée aux inspecteurs de la sécurité des navires, agents de l'État spécialistes de sécurité maritime, qui devront s'approprier les idées essentielles de la cybersécurité pour pouvoir auditer les systèmes de gestion de la sécurité des compagnies et effectuer les contrôles à bord de manière pertinente.

L'idée que la cybersécurité serait avant tout une affaire de spécialistes, de traqueurs de lignes de code malveillantes, est non seulement erronée mais dangereuse. Elle occulte une réalité, celle de l'importance cruciale de la compréhension par chacun des risques que l'informatisation et la numérisation des métiers a fait naître jusque dans les tâches les plus banales du quotidien. Le concept de « facteur humain » est si rabâché qu'il en est devenu un truisme. Il n'en comporte pas moins ce fond de vérité essentielle que rien ne s'accomplit sans l'adhésion de tous et sans une compréhension minimale de ce que la sécurité signifie pour chacun. D'où la nécessité du dialogue. Pas seulement celui des machines et des serveurs. Pas seulement la sacro-sainte interopérabilité des systèmes. Ce sont d'abord des humains qui doivent apprendre à parler le même langage.

[1] Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer
[2] Convention internationale pour la prévention de la pollution par les navires
[3] Organisation maritime internationale
[4] Code international pour la sûreté des navires et des installations portuaires (rattaché à la convention SOLAS)
[5] Code international de la gestion de la sécurité (rattaché lui aussi à la convention SOLAS)
[6] Baltic and International Maritime Conference (association regroupant de nombreux armateurs et professionnels du secteur maritime)

Un secteur uni pour faire face au risque cyber

BRUNO BENDER
Coordonnateur cybersécurité maritime, Comité France Maritime

A l'instar de la mer, le cyberespace est un espace de liberté et d'échange pour ceux toujours plus nombreux qui y évoluent. Milieu infini dont les richesses attirent l'attention des uns et les convoitises des autres, l'espace numérique se caractérise par une certaine abstraction qu'il est aujourd'hui nécessaire de matérialiser de sorte que les décideurs puissent mieux en saisir les enjeux. Liées aux priorités stratégiques (commerce, finance, transports, culture, défense…) les données qui circulent dans l'espace numérique font l'objet de nombreuses convoitises. Milieu infini, propice à l'anonymat, il se caractérise par sa similitude avec le milieu maritime. Comme lui le cyberespace est un espace d'échanges, d'influence, ou l'on se mesure et on s'affronte pour s'approprier les richesses qui y évoluent. La protection pleine et entière de ce milieu est une utopie. Celle des données qui y évoluent est une nécessité - sans que cette protection ne se transforme toutefois en entrave.

L'approche trans-sectorielle de la sécurité

L'Union Européenne a approuvé en 2014 une stratégie de sûreté maritime (SSMUE) qui constitue une déclinaison de la stratégie européenne de sécurité pour le domaine maritime. Insistant sur le décloisonnement entre les acteurs et une optimisation de l'existant, elle propose une approche trans-sectorielle fondée sur la complémentarité des instruments et des politiques, militaires et civils, maritimes et portuaires assurant le continuum entre sécurité intérieure et extérieure et garantissant l'autonomie décisionnelle de l'Union. La stratégie nationale de sûreté classe les menaces qui pèsent sur le monde maritime en trois grandes catégories:

- Celles liées aux activités maritimes, telle la piraterie, qui ont toujours existé mais se sont accrues avec le développement du trafic maritime ;

- Celles existant à terre qui se sont « maritimisées » ;
- Celles spécifiquement liées à la part croissante du numérique liés aux nouveaux espaces de contestation extra-atmosphériques et numériques.

Les systèmes connectés du monde maritime sont exposés comme les autres, à la malveillance numérique. La possibilité pour des hackers de prendre le contrôle sur les moyens de communication de navires, de créer de faux navires, d'émettre de faux messages voir de désactiver les systèmes de sécurité a été démontré à de maintes reprises.

De façon plus directe, la cybersécurité aujourd'hui peut tuer une personne, détruire une installation, contribuer à désorganiser une activité commerciale ou atteindre notre vie privée au quotidien. La dépendance au numérique du secteur maritime constitue un démultiplicateur de l'efficacité des opérations. Le revers de cette numérisation est l'impérative nécessité de la cybersécurité pour la protection des données et la stabilité des réseaux soumise à l'attaque d'individus, mais aussi d'états.

L'augmentation significative des attaques en 2020

Nous connaissons tous l'attaque subie par Maersk en 2017 et celles plus récentes sur CMA-CGM, GEFCO, MED EUROPE TERMINAL, MSC, l'Organisation Maritime internationale en 2020. Le tableau ci-après décrit de façon sommaire les attaques les plus importantes subies par les acteurs du monde maritime au cours des dernières années. Il donne quelques enseignements à partir d'observations faites et de quelques rares rapports. Contrairement aux pays nordiques, les compagnies attaquées, en France, ont encore du mal à communiquer sur le sujet.

La menace est omniprésente sous diverses formes et peut représenter un acte de guerre. En mars 2020, c'est Israël qui a revendiqué une attaque sur les systèmes du terminal portuaire de « Shahid Rajaee » à Bandar-Abbas dans une zone extrêmement sensible à proximité du détroit d'HORMUZ. L'attaque a entraîné une incapacité temporaire pour le port de fonctionner et a entraîné une série de contre-attaques de la part de hackers iraniens.

La filière maritime fait le constat, comme d'autres, d'une augmentation

significative du nombre d'incidents. Ceux-ci se ont touché des entreprises déjà fragilisées par ailleurs pendant la crise COVID. Leur quantification reste difficile en raison du manque de données précises (les opérateurs ne remontent pas toujours les incidents et la filière maritime ne dispose pas à ce jour d'outils capables de fournir ces indicateurs). Un opérateur israélien[1] (*Naval Dôme*) a estimé une augmentation de 400% du nombre d'attaques au 1er trimestre 2020.

Etats voyous et organisations criminelles souvent à la manœuvre

Le monde maritime a depuis toujours été un espace d'affrontements, entre nations de façon directe parfois, mais souvent par l'intermédiaire de pirates et de corsaires, dans des zones souvent reculées. Une menace semblable s'est développée dans les profondeurs du web de façon anarchique par quelques individus mais également pilotée, voire savamment orchestrée par des organisations criminelles et des états.

La cyberdélinquance est susceptible aujourd'hui de provoquer des dégâts bien plus importants sur nos économies - c'est là aussi tous les jours un peu plus vrai dans un domaine maritime en pleine numérisation.

Aujourd'hui pour l'ensemble des secteurs économiques, le numérique est un facilitateur des opérations mais c'est aussi un outil au service des acteurs malveillants comme facilitateur de la commission de leurs délits. La crise COVID en 2020 et le recours massif aux outils numériques n'a fait que confirmer la dépendance croissante aux outils numériques et le besoin pour le secteur maritime de s'organiser pour sa défense. Faire l'impasse sur sa sécurité numérique c'est mettre en danger son activité.

La sécurisation des espaces de liberté que sont la mer et le cyberespace nécessite une action globale.

Si sur les mers les pirates agissent de façon traditionnelle avec des armes classiques et des méthodes rudimentaires mais éprouvées, il ressort que dans le cyberespace les systèmes connectés et leurs supports offrent une exposition bien plus grande et permettent une forte évolutivité des modes d'actions.

Cette sensibilité est d'autant plus avérée sur des systèmes maritimes eux-mêmes porteurs de données directement liées aux richesses transportées. La cyberdélinquance dans le domaine reste donc principalement économique, dans le but de s'approprier de façon illégale une richesse à partir des données volées ou des failles exploitées. Mais l'attaque du port de Bandar Abbas et celle plus ancienne des centrales d'enrichissement d'Uranium par les Etat-Unis (attaque par le Ver STUXNET en 2010) marquent également un retour d'actes de guerre là aussi par tiers interposés.

Une politique coordonnée en matière de cybersécurité maritime.

La cybersécurité est de mieux en mieux prise en compte dans le monde maritime, il y a de plus en plus d'initiatives et d'instances, mais elles sont divisées, éparses et limitées dans leur périmètre et dans leurs compétences. Elles peuvent servir de base pour la mise en place de solutions mais doivent être fédérées.

Autour d'une gouvernance partagée et du futur centre de coordination de la cybersécurité, l'ensemble des forces vives du domaine du maritime se mettent aujourd'hui en ordre de bataille pour coordonner leur action et définir une stratégie pour les professionnels, et avec les acteurs industriels.

La création d'une offre française structurée, adaptée à la filière maritime garantira la fiabilité des personnes, la résilience des systèmes et la protection des informations face aux menaces. Pour ce faire, les acteurs publics et privés doivent structurer leur réponse de façon adaptée et cohérente sur des aspects à la fois techniques, organisationnels et humains. La cybersécurité ne doit pas seulement être vécue comme une contrainte, elle doit être une opportunité, un facteur de différenciation pour nos entreprises et pour nos ports dans une concurrence internationale de plus en plus exacerbée.

[1] Naval Dome: https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/

Le port du futur sera un port « smart » et cyber sécurisé !

JÉRÔME BESANCENOT
Chef du Service du développement des Systèmes d'Information,
HAROPA Port du Havre

Le secteur portuaire : une dépendance au numérique, une interdépendance face au risque cyber

Face à la massification du transport maritime, un facteur clé de la compétitivité des ports repose désormais sur la capacité de leurs systèmes d'information à automatiser et traiter de volumineux flux d'information liés aux marchandises, aux passagers et aux navires.

Ces traitements sont opérés au travers du système d'information portuaire communautaire appelé communément « Port Community System » (PCS) et reposent sur des échanges dématérialisés de données en EDI de type BtoB interconnectant l'ensemble des parties prenantes de la communauté portuaire. Le volume échangé représente plusieurs centaines de millions de transactions par an pour le port du Havre.

La communauté du port rassemble de nombreux professionnels des secteurs portuaires, maritimes et aussi industriels ; de par sa nature, elle se caractérise par une grande disparité de sensibilisation et de culture face au risque cyber. Chaque acteur intervient de manière synchronisée dans la chaîne d'approvisionnement logistique : l'ensemble des opérations est coordonné par le biais du PCS. Ceci induit de fortes interdépendances entre les professionnels, en matière de règle d'hygiène cyber ; il s'avère fondamental de partager les bonnes pratiques numériques pour sécuriser l'ensemble de l'écosystème.

Cette dépendance de l'activité portuaire au monde numérique s'est considérablement accrue ces dernières années, du fait de l'automatisation qui

est devenue une nécessité économique et un enjeu de performance. Le recours aux nouvelles technologies permettant de réduire les coûts, de fiabiliser le suivi des opérations portuaires et de mieux anticiper les interventions des acteurs de la logistique. À ce titre, le concept du « SmartPort », présente un port « hyper-connecté » s'appuyant sur les technologies de l'internet des objets (IoT), sur le bigdata et sur l'intelligence artificielle (IA) qui laisse augurer une plus grande agilité due au pilotage de l'activité par la donnée numérique. Dans le même temps, l'augmentation de la surface d'exposition aux cybermenaces et du risque de leur propagation est le revers de la médaille.

Il devient donc nécessaire de s'extraire d'un fonctionnement qui reposerait uniquement sur une analyse en silo des risques de cybermalveillance, en combinant les analyses et en partageant davantage au niveau de la communauté portuaire une même stratégie globale de résilience de l'écosystème. Dans cet objectif, il convient de mettre en oeuvre une véritable synergie de place afin d'amener l'ensemble des acteurs à se pencher conjointement sur ce sujet sensible, trop souvent considéré comme une affaire de spécialistes en informatique et rarement appréhendé sous sa dimension organisationnelle.

Force est de constater que le secteur portuaire n'est plus épargné par les cyberattaques et certaines d'entre elles ont récemment eu de lourdes conséquences pour plusieurs ports mondiaux majeurs, notamment sur le plan financier et la continuité d'activité.

Le Programme « SmartPortCity » de HAROPA Port du Havre : un projet innovant en matière de cybersécurité portuaire

Pour faire évoluer les lignes favorablement et pour se mobiliser de manière proactive sur ce sujet complexe, HAROPA Port du Havre a initié, au sein du programme « SmartPortCity », lauréat du TIGA-PIA3 (Territoires d'Innovation Grande Ambition - Plan d'Investissement d'Avenir), un projet d'innovation en matière de cybersécurité portuaire, maritime et industrielle avec l'ensemble des parties prenantes du territoire havrais dont la communauté Urbaine Le Havre Seine Métropole, la communauté des

professionnels portuaires de l'UMEP (Union Maritime et Portuaire), les industriels de l'association Synerzip et la SOGET leader mondial de solution PCS et éditeur de la plate-forme collaborative digitale S)One.

Le port du Havre est le premier port à conteneurs pour le commerce extérieur de la France et aussi le 1er port touché sur le range nord-européen. Il offre les meilleurs temps de transit entre l'Europe et le reste du monde et se positionne comme un corridor européen majeur. Localisé à l'embouchure de la Seine, il est relié directement aux ports de Rouen et Paris par route, fleuve et rail. Ces trois ports sont désormais regroupés sous HAROPA, portant une ambitieuse stratégie de développement et d'innovants services digitaux à l'échelle territoriale de l'axe seine. Dans ce contexte, la sûreté est une orientation clé pour HAROPA – Port du Havre qui est la première autorité portuaire européenne à avoir obtenu la certification ISO 28000 au titre de la sûreté de la chaine d'approvisionnement.

Le projet de plateforme de cybersécurité portuaire, maritime et industrielle vise à poursuivre cette stratégie de renforcement du port dans une dimension de compétitivité et d'attractivité, tout en assurant une amélioration du niveau général en matière de cybersécurité avec un enjeu double.

Le premier enjeu consiste à bâtir une démarche qui apportera de la visibilité aux clients du port sur le dispositif déployé de résilience de l'écosystème aux cybermenaces. Comme un service à valeur ajoutée au bénéfice de ses clients, le port améliorera sa compétitivité justement du fait de la prise en compte de la dimension cyber dans sa stratégie de développement. Cet enjeu est caractérisé par une image forte de construction « du Havre : port Cyber-sûr ». Il ne s'agit pas seulement d'identifier ce que le port pourrait « perdre » en cas de non-conformité cyber, mais plutôt de souligner ce qu'il gagne et la façon dont cet argumentaire devient un élément de décision susceptible d'apporter des trafics et de l'activité au port du Havre.

Le deuxième enjeu est d'aller au-delà de la stratégie de résilience en développant une culture d'innovation sur la cybersécurité portuaire, maritime et industrielle. Cela consiste à élargir les compétences des acteurs et à attirer de nouveaux talents sur le territoire dans cette discipline. Il s'agira essentiellement d'impliquer les acteurs pour créer une valeur ajoutée de type

filière sur la promotion des métiers de la cybersécurité et favoriser ainsi la mise en oeuvre de partenariats public-privé (PPP) dans ce domaine. L'idée est de susciter auprès de différents acteurs du monde numérique et de la recherche en cybersécurité, une meilleure prise en compte de la « Security by design » dans le développement informatique des solutions portuaires, dans la certification des installations technologiques, ou encore un meilleur niveau de formation initiale et continue. Cet enjeu vise à améliorer l'attractivité du territoire et à contribuer à fixer un savoir-faire local en faisant « du Havre le lieu d'amélioration de la cybersécurité » de ses entreprises.

La cybersécurité, un facteur de compétitivité pour HAROPA Port du Havre et pour l'écosystème portuaire français

Le calendrier du projet a été défini pour établir en première priorité la gouvernance cyber de la plateforme en déclinant de manière opérationnelle des mesures pragmatiques, adaptées aux besoins du port et répondant à une gestion raisonnée des vulnérabilités : le piège d'une potentielle distorsion de concurrence avec d'autres ports devra être écarté, en s'assurant en permanence que les mesures adoptées ne soient pas disproportionnées ou trop difficiles à porter. Chaque entreprise, quelle que soit sa structure ou son organisation, deviendra alors un acteur essentiel de cette gouvernance et participera à son animation. Dans cette perspective, les évènements organisés depuis 2018 au Havre, en partenariat avec le CyberCercle, en faveur de la sûreté portuaire et la sécurité numérique, ont permis avec succès de sensibiliser l'ensemble des acteurs de la place portuaire sur des thématiques de réglementation, de sensibilisation, de gouvernance ainsi que d'innovation.

En parallèle, un échéancier pour les trois ans à venir, sur la base de cette gouvernance, va établir une feuille de route de création d'un portefeuille de services mutualisés d'assistance aux entreprises comprenant de la sensibilisation, de la formation, de l'analyse et des audits de risque, de la gestion de crise, de la recherche et innovation, un SOC portuaire (Security Operation Center) et une place de marché pour faciliter l'accès aux offres techniques de sociétés cyber-spécialisées reconnues.

La clé du succès du projet repose ainsi principalement sur la capacité collective

à valoriser véritablement cette initiative sous l'angle du progrès, en dépassant le stade simpliste où elle ne serait perçue que selon son principe d'obligation réglementaire. La cybersécurité peut alors être appréhendée comme une opportunité permettant au port d'améliorer sa compétitivité en combinant l'accélération de la transformation digitale et sa sécurisation numérique. Elle devient alors un critère positif, et donc, un argument commercial garantissant la « compliance » de l'écosystème portuaire havrais. Cette « compliance » va pouvoir se valoriser auprès des entreprises de la place, en termes d'attractivité auprès des clients du port, permettre potentiellement de conquérir des parts de marché ou plus pragmatiquement par exemple, de réduire les primes d'assurances des entreprises du territoire.

Ce projet ambitieux revêt aussi une dimension d'intérêt général, car il est essentiel que le modèle défini et mis en place puisse être dupliqué sur d'autres territoires au niveau national comme à l'international. Il devra notamment pouvoir s'adapter aux différents contextes, en se déclinant aux besoins des ports plus petits où les moyens d'action font face à des contraintes fortes de moyens. Il s'inscrira aussi dans la politique nationale et européenne en matière de cybersécurité maritime en étroite collaboration avec le Secrétariat Général de la Mer (SGMer) où l'interopérabilité de la plateforme de cybersécurité portuaire, maritime et industrielle avec le futur M-CERT (Maritime - Computer Emergency Response Team) national est un enjeu clé du dispositif.

En résumé, HAROPA Port du Havre au travers d'une inédite démarche d'innovation s'engage sur un processus de progrès pour renforcer sa politique en matière de cybersécurité portuaire, maritime et industrielle, faisant de cette discipline un vecteur essentiel du développement de l'activité du port et de sa résilience. Cette initiative permettra aussi à l'État d'affermir sa souveraineté nationale en intégrant le « Port Cyber sécurisé » dans son dispositif global de cybersécurité maritime, contribuant ainsi à sécuriser le commerce international sur le moyen et long terme.

Le rôle de la construction navale en matière de cybersécurité maritime

JEAN-MARIE DUMON
Délégué Général adjoint, GICAN

Le monde maritime a mis du temps à prendre conscience de l'importance croissante de la cybersécurité pour la maîtrise des défis actuels et futurs qu'il doit affronter.

Et pourtant le cyberespace présente bien des aspects de similitude avec l'océan, avec ses objets isolés, répartis ou interdépendants, ses flux permanents ou localisés. Il possède de nombreuses couches qui n'ont rien à envier à la complexité des fonds abyssaux. Mais cet espace va encore plus loin dans son interaction avec la pensée humaine avec les notions de couches supplémentaires comme la Noosphère, chère à Pierre Teilhard de Chardin et Vladimir Vernadski.

Les marins développent donc des aptitudes favorables à des problématiques de ce type et savent affronter les menaces, naviguer sur l'avant et parer les avaries pour mener à bon port la cargaison.

Ceux qui construisent et équipent les navires possèdent la lourde responsabilité d'intégrer la dimension cyberspatiale dans la conception, la construction et le maintien en condition tout au long du cycle de vie de ceux-ci. La réponse aux cyberattaques et l'intégration « by design » des dispositions de cybersécurité deviennent dans ces conditions la norme.

La cybersécurisation des espaces maritimes se nourrit de ce qui se joue « à terre », en mer et à bord. Si la prise en compte d'une des trois dimensions est insuffisante, le résultat obtenu sera en deçà des attentes et la perméabilité aux attaques probable.

Tout d'abord, ce qui se passe à terre, peut se déclencher en mer. Le continuum « terre-Mer » en matière de cyber est de plus en plus marqué. Le fait d'être en mer n'offre aucune protection. Les flux ne cessent d'augmenter et les vecteurs d'attaques sont maintenant souvent aussi agiles dans les espaces maritimes qu'ailleurs. D'ailleurs, le type d'attaque proféré sur le segment maritime n'est pas fondamentalement différent de celui qui s'exerce à terre et les virus informatiques les plus courants ont aussi droit de cité.

Ensuite, l'interdépendance des activités humaines dont le dénominateur est l'espace océanique ne cesse de se renforcer. Cet effet de sphère conduit à se voir développer des occurrences de risques spécifiques à l'environnement maritime, qui apparaissent de manière discrète au sens mathématique, mais qui profitent de l'effet nodal et du contournement des architectures. Ainsi, La cybersécurité du maritime est dépendante des activités spatiales, météorologiques, industrielles, portuaires, de transports multimodaux, de l'exploitation minérale ou halieutique et de bien d'autres facteurs ce qui crée des occurrences exponentielles.

Enfin, à bord des navires, il a fallu penser ou prendre en compte la numérisation de ceux-ci et s'affranchir d'idées reçues « physiques » pour développer une approche d'abord digitale pour répondre aux enjeux de cybersécurité embarquée. Le capitaine d'un navire pense que la richesse de celui-ci, ce sont ses passagers, son soja ou ses containers, et qu'il doit donc les protéger. Le commandant d'un bâtiment de guerre pense avant tout à sa capacité de combat et donc à ses senseurs et ses armes. Le risque cyber est donc d'être aveuglé par ces paramètres immédiats de valeur et de vouloir les protéger, sans comprendre que les fragilités cyber sont peut-être ailleurs et peuvent d'abord être perméables au sein de parties moins essentielles du navire.

La construction navale au centre des enjeux de cybersécurité

Le rôle de la construction navale en matière de cybersécurité maritime est fondamental car les entreprises qui y contribuent sont au cœur du sujet, depuis la forme de construction jusqu'aux confins des océans. Elles connaissent la menace, les vulnérabilités et construisent les solutions.

Le chantier naval constitue le siège d'une combinaison industrielle hors-norme avec des risques parfois insoupçonnables. La longueur du temps de construction, le volume des équipes de techniciens et ouvriers, la coactivité extrêmement contraignante et l'augmentation des niveaux de sous-traitance multiplient les particularismes à prendre en compte. Un sous-marin nucléaire est à la fois une base de lancement de fusée, une centrale nucléaire, un data center, une cité autarcique avec ses services, un objet mimétique du milieu sous-marin et un atelier industriel. Comment penser la cyber sécurité dans de telles conditions ? Le chantier naval est donc un consommateur de cybersécurité, qui tient compte de l'objet construit, ce qui n'est pas une mince affaire compte-tenu de l'interconnectivité grandissante et de l'empilement de systèmes collaboratifs, voire de systèmes de systèmes. L'industrie est la seule à pouvoir appréhender la complexité des flux et leur importance. La capacité d'intégrer garantie celle de mettre en place des dispositions de cybersécurité performantes.

La digitalisation croissante des procédés industriels conduit à concevoir différemment les navires et finalement à construire pas à pas le jumeau numérique du produit. L'industrie navale a pu ainsi proposer progressivement des navires « cyber by design ».

De consommateur en cybersécurité, l'industrie navale a des atouts indéniables pour être producteur de cyber solutions. Elle connait les fragilités, les sources de vulnérabilité, les normes applicables selon les clients et surtout bénéficie du retour d'expérience des technologies duales par l'activité du naval de défense.

Les exigences de cyberdéfense sur un navire de combat de premier rang permettent d'évaluer des solutions durcies qui rendent inopérantes des attaques complexes, massives ou spécifiques. L'apprentissage de ces sujets, la collaboration avec les centres techniques de « maitrise de l'information » de la Direction Générale de L'Armement, ont fait progresser les industriels du naval.

Le besoin de sécuriser les sites industriels d'importance vitale et d'avoir une approche portuaire dans la cybersécurité a stimulé l'excellence des produits développés par nos entreprises.
Le besoin encadrant de la cyberdéfense pour le naval, la perception des

nouvelles menaces de souveraineté et la politique de sécurité des activités d'importance vitale sur l'ensemble de la chaîne de valeur maritime et portuaire, ont permis de se doter d'outils de lutte de grande qualité.

Mais la question centrale est bien de disposer d'une offre répondant aux besoins de l'ensemble des acteurs économiques et la grande qualité de nos entreprises du secteur a été d'adapter et d'évoluer en conséquence. Il ne s'agit pas uniquement de prêter attention aux Opérateurs de Services Essentiels (OSE) au sens de l'application des directives européennes Network Information Security (NIS), car ils ne sont pas forcément bien appréhendés en France, du fait du manque d'association des acteurs industriels à la question, mais bien de trouver un équilibre entre le coût et le bénéfice des dispositions de cyber sécurisation.

Quelle réponse à l'avenir ?

L'industrie navale voit son action évoluer au fur et à mesure, comme la mentalité et la perception d'une accélération des cybermenaces l'y invitent.

Le navire n'est plus isolé et un ransomware à bord peut infecter toute la chaîne logistique d'une compagnie maritime, et les clients de celle-ci. Le dénominateur commun du navire reste le pivot de la démarche.

Les réponses sont multiples et à la mesure des enjeux.

Le coût d'une attaque devient donc prohibitif et l'industrie navale s'est résolument tournée dans les stratégies de filière qui permettent à l'Etat et au secteur privé de fédérer leurs initiatives, de financer la recherche, de soutenir l'action internationale et la bataille de l'emploi, de plus en plus importante pour notre secteur.

La cybersécurité est un des projets de filière pour l'industrie de sécurité. Le GICAN est un des membres fondateurs de cette filière car il estime que le particularisme maritime offre un terrain favorable aux projets d'envergure et qu'ils peuvent se combiner avec la logique des territoires de confiance pour les aspects portuaires et de la sécurisation des grands événements, pour les aspects nautiques et fluviaux.

Dans le même temps, la filière des industriels de la mer souhaite développer sa stratégie autour de la numérisation du chantier naval, de son développement dans une optique 4.0 et de la conception de solutions « smart » pour les navires de nouvelle génération. Derrière tous ses axes se profilent des aspects de cybersécurité omniprésents et devant être impérativement considérés à leur juste niveau. Le Conseil d'Orientation de l'Innovation en Mer (CORIMER), dans son travail de labellisation, est l'enceinte de recueil des appels à manifestation d'intérêt pour la feuille de route de la filière des industriels de la mer. Trop peu de projets, spécifiquement sur les technologies cyber, y sont présentés, alors qu'ils pourraient avoir du sens dans une logique multisectorielles et avant tout maritime, mais la pédagogie et la prégnance des menaces fera évoluer la perception. En effet, cette filière rassemble l'industrie navale, le nautisme, l'offshore pétrolier et les énergies marine renouvelables. Les débouchés sont donc bien réels et les plateformes d'activité en mer et les câbles sous-marins méritent une cyber sécurisation du même ordre que l'ensemble de la filière maritime.

Le GICAN développe, de plus en plus, une logique d'écosystème, au côté d'une perception industrielle et patronale. A cet effet, il accueille en son sein les sociétés de classification et le monde assurantiel. Il est indéniable que la cybersécurité maritime est en retard en matière de réglementation ou de normalisation internationale car c'est le lot des sujets traités au sein de l'Organisation Maritime Internationale (OMI) pour tout sujet devant déboucher sur un consensus des grandes nations maritimes. Il est donc d'autant plus important que la couverture du risque cyber et la normalisation de la classification des navires dans ce domaine fassent partie des préoccupations du secteur maritime en France. En effet, il s'agit d'une véritable bataille et les choix qui seront faits conditionneront la maîtrise de la conception des outils cyber. Faire valoir les solutions de nos entreprises est un enjeu de souveraineté.

La réponse cyber dépend aussi de la faculté d'agréger les compétences vers un même objectif. Nous avons la chance en France d'avoir pu mettre en place, avec d'autres, le Centre de Coordination de la Cybersécurité du Monde Maritime (C2M2). Cela permet de traiter les sujets de la connaissance de la menace, de la meilleure anticipation, de la surveillance, de la gestion des incidents, de la formation en matière de cyber et de l'interopérabilité sous

bien des aspects. Demain, cette impulsion nous permettra d'être en situation de jouer un rôle majeur à l'échelle européenne.

Enfin, les crises systémiques, comme la crise sanitaire de la COVID, doivent nous faire réfléchir à la fragilité de notre écosystème maritime. L'impasse sur la sécurité numérique est une tentation dangereuse quand les difficultés économiques s'accumulent et en particulier pour les PME agissant dans ce champ. Les strates complexes de la supply-chain dans l'industrie navale rendent nécessaires l'accompagnement et l'aide à prodiguer pour la mise en place de solutions de cyber sécurité efficaces pour leurs activités.

Lutte contre la cybercriminalité maritime : Prévôts de la mer contre pirates

STEPHANE FRONCZAK
Chef de la cellule CYBERGENDMAR, Gendarmerie Maritime

La piraterie est un corollaire du commerce maritime et existait déjà dans l'Antiquité. Toutes les civilisations anciennes ayant possédé une marine l'ont pratiquée, les Phéniciens comme les Mycéniens.[1]

Depuis l'Antiquité, l'espace maritime a donc été un lieu d'enrichissement, au profit de criminels (pirates), de serviteurs d'Etats (corsaires), de Nations (flotte de guerre), d'acteurs privés (armements / compagnies).

Les pirates existent depuis que la navigation existe. La piraterie n'est ni plus ni moins que du brigandage des mers.

Le mot pirate vient du mot grec πειρατης qui vient à son tour du verbe πειραω (puis du latin Pirata) signifiant « s'efforcer de », « essayer de », « tenter sa chance à l'aventure ».[2]

Par analogie, un pirate informatique désigne un individu s'adonnant à des détournements de fonds, à l'acquisition de biens, de données ayant une forte valeur ajoutée, effectués par Internet, ou des copies d'oeuvres sans respecter le droit d'auteur ou le copyright. Il en existe d'autres formes plus crapuleuses comme l'hameçonnage, qui consiste à usurper une identité, le plus souvent Corporative. Citons enfin le phishing, la demande de rançon (ransomware), ou le social engineering.

Les cybercriminels sont donc les dignes héritiers d'une tradition maritime ayant aujourd'hui pour espace de navigation, l'Internet, les réseaux. Jamais la mixité cyber et maritime n'a été aussi vrai d'un point de vue économique.

Après nous être intéressé aux raisons de cette cyber-convoitise maritime, défini les enjeux économiques et stratégiques, puis précisé rapidement le cadre d'une réglementation au nécessaire dimensionnement international, nous aborderons les spécificités du cyber maritime, avant d'évoquer un historique des attaques cybercriminelles ayant un lien avec le monde maritime. Puis nous terminerons sur les enseignements de ces attaques ayant conduit les professionnels de la mer à réfléchir, à se mettre en ordre de bataille pour affronter ce qui est aujourd'hui une évidence : les pirates informatiques (de tous ordres, terroristes compris) vont déployer les outils et stratégies qu'ils ont patiemment élaborés afin de s'enrichir, compromettre, le plus important secteur économique du commerce mondial.

Ce postulat constituera notre conclusion qui s'enrichira de ce qui est à la fois le nouveau défi technologique maritime d'un futur existant et un enjeu cyber sécuritaire : le navire autonome.

En avant-propos, il me semble utile de préciser aux néophytes en la matière cyber, la distinction sémantique à faire entre cyber sécurité et cyber criminalité.

Sans redéfinir ce qui existe déjà, on peut exposer que la cybersécurité est la protection des systèmes informatiques connectés à l'Internet (et aux réseaux), contre les menaces informatiques visant le matériel, les logiciels et les données. L'objectif de la cybersécurité est de limiter les risques et de protéger le parc informatique d'assaillants aux intentions malveillantes. La sécurité informatique, qui consiste à maintenir la confidentialité, l'intégrité et la disponibilité des données, est un sous-ensemble de la cybersécurité.[3]

La cybersécurité permet de prévenir au mieux les atteintes aux données, les vols d'identité ou encore le piratage par rançongiciel.

La cybercriminalité est l'ensemble des infractions pénales (cybercrimes) commises par le biais de l'Internet ou des réseaux informatiques. La cybercriminalité se déroule donc dans le cyberespace. Elle comporte des infractions très variées :

- Piratage informatique, intrusion dans des ordinateurs, dans des serveurs informatiques ou dans des sites Internet ;

- Destruction à distance de données informatiques ;
- Fraudes à la carte bancaire par Internet ;
- Traitements automatisés de données personnelles non autorisés ou non déclarés ;
- Création de faux sites Internet imitant des sites connus (par exemple un faux site Internet de telle enseigne commerciale) ;
- Pédopornographie (sites Internet pédopornographiques, par exemple) ;
- Incitation à des délits contre les personnes ou contre les biens, par le biais d'Internet.

Les enjeux économiques de la cyber convoitise maritime du 21ème siècle

Le transport maritime assure près de :
- 90% des échanges mondiaux*
- 74% du commerce européen*
- 78% des importations françaises*
- La France = 2ème domaine maritime mondial. Soit 643 427 km² de superficie de côtes, c'est-à-dire 4668 kms de longueur de côte.[4]
- 11 millions de km2 de zone économique exclusive (outre-mer inclus)
- Economie maritime : 1500 Mds € (en plein expansion) – 60.000 navires de commerce (1000 unités FR) – 90% du fret international – 334 millions de tonnes transportées - 50 % des communications – 28,3 millions de passagers en 2017 (Src Service de la donnée et des études statistiques – Commissariat général au développement durable - 2018)

Exemples de statistiques portuaires :
- Fréquentation portuaire Méditerranée : 11 millions de passagers ;
- Total des passagers croisiéristes en 2017 : 4,2 millions ;
- Transport de containers : +88% depuis 2001 ;

Zones portuaires ISPS : Brest – Toulon – Marseille – Le Havre – Port de Bouc – Cherbourg – Calais – St Nazaire

Il apparaît dès lors que les enjeux économiques en présence sont de nature à susciter des convoitises que le cyber ne saurait ignorer. Tout récemment encore (14/03/2020) la métropole Marseille / Aix en Provence a fait l'objet

* Source : Commission européenne

d'une cyber attaque au ransomware d'une ampleur inégalée. Un dommage collatéral de cette attaque a été réalisé auprès d'une société filiale d'une grand groupe français du domaine maritime qui a vu ses PC être cryptés. Une enquête est en cours.

La liaison est idéale pour vous exposer une législation pénale qui a dû se réinventer, depuis bien des années, au regard d'une technologie très évolutive. Et par conséquent, une cybercriminalité aux multiples visages.

Il faut tout d'abord prendre en considération le fait que les enjeux sont tels que la préservation de ces outils économiques maritimes est apparue comme une priorité pour le législateur et les acteurs de la sécurité informatique de notre pays. Ainsi les zones portuaires évoquées supra, les grands armements français ont été définis comme OIV (article R. 1332-1 du Code de la Défense – Loi de programmation militaire 2014-2019) ou OSE (Proposition de l'ANSSI et validation par le 1er ministre). La directive NIS[5] coordonnant les actions conduites en matière de sécurité au niveau européen.

En matière de répression pénale, la lutte s'organise depuis 10 ans. Sans faire un inventaire « à la Prévert », je retiens ces textes majeurs[6]:

- Perben II : La loi du 9 mars 2004 portant sur l'adaptation de la justice aux évolutions de la criminalité afin de lutter contre la « délinquance et la criminalité organisée ».
- Loppsi 2 (loi d'orientation et de programmation pour la performance de la sécurité intérieure)
- LPM (Loi de Programmation Militaire n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025)
- Loi anti-terrorisme / Loi sur le Renseignement

Abordons les risques cyber, avant d'évoquer un historique des attaques cybercriminelles ayant un lien avec le monde maritime.

La nature des risques de sécurité et des APTs (menace persistante avancée) évolue constamment, ce qui constitue un vrai casse-tête pour assurer la cybersécurité, au niveau terrestre comme maritime.

Les menaces à la cybersécurité peuvent prendre plusieurs formes :

- Malware : type de logiciel malveillant dans lequel n'importe quel fichier ou programme peut être utilisé pour porter préjudice à l'utilisateur d'un ordinateur, que ce soit par un vers, un virus, un cheval de Troie ou un logiciel espion.
- Rançongiciel (ransomware) : type de malware par lequel un attaquant bloque l'accès aux fichiers système de l'ordinateur de la victime - souvent par cryptage - et exige une rançon pour révéler le code et débloquer l'ordinateur.
- Ingénierie sociale : méthode qui repose sur l'interaction humaine pour tromper l'utilisateur et contourner les procédures de sécurité afin d'accéder à des informations sensibles, généralement protégées.
- Hameçonnage (phishing) : type de fraude qui consiste à imiter des courriels provenant de sources de confiance. L'objectif de ces messages est de voler des données sensibles telles que le code d'une carte de crédit ou des informations de connexion.

Nous pouvons malheureusement illustrer l'action cybercriminelle au monde maritime sans rechercher trop loin. Souvenons-nous :
25 juin 2015 : La société SABELLA immerge la première hydrolienne productive à 2kms au large de Ouessant.

Octobre 2015 : attaque virale sur les serveurs de communication de la turbine SABELLA, neutralisant pendant quinze jours la connexion avec le centre de contrôle. L'attaque était accompagnée d'une demande de rançon.

Juin 2017 : Maersk a été l'une des premières victimes de grande envergure maritime de l'épidémie Petya Not Petya (wannacry). 300 millions de dollars de pertes.
"Imaginez une entreprise où un navire de 10 à 20.000 conteneurs entre dans un port toutes les 15 minutes, et pendant 10 jours, vous n'avez pas d'informatique « (PDG de Maerks).
Nota : En France, ont été impactés Auchan, la SNCF et Saint Gobain.

Septembre 2018 : les ports de Barcelone et San Diego pris pour cibles.
Le premier à avoir été touché a été le port de Barcelone, en Espagne, le 20 septembre. La deuxième attaque a été signalée le 25 septembre par le port de

San Diego, aux États-Unis. L'impact recherché était d'une part la neutralisation des opérations commerciales entre les compagnies et leurs navires. But non atteint. Le second objectif était d'obtenir un ralentissement sur l'ensemble des opérations terrestres telles le déchargement et chargement des navires. But atteint.

2019 : Les armements, compagnies maritimes et les entreprises portuaires en lien avec l'activité économique maritime n'échappent pas aux trois types de cyberattaques les plus courantes. L'étude du CESIN[7] dresse également un état des lieux des types d'attaques informatiques qui visent le plus souvent les entreprises françaises. Comme les années précédentes, c'est le phishing ou spear-phishing (hameçonnage) qui est en tête des attaques les plus couramment constatées.

Cette fraude a été signalée par 79 % des entreprises piratées l'année dernière. L'arnaque au président constitue également une arnaque à la mode ces derniers temps puisqu'elle a touché environ la moitié des entreprises ciblées en 2019.
Cette escroquerie consiste, pour l'escroc, à se faire passer pour le dirigeant d'une entreprise et à obtenir un virement.
Le rapport d'activité 2019 de cybermalveillance.fr dresse également un constat similaire et plus complet.[8]

Les cyberattaques les plus courantes contre les entreprises

Types d'attaques les plus constatés par les entreprises françaises en 2019**.** Plusieurs réponses possibles, sélection des résultats supérieurs à 20%. En moyenne : 3,9 types d'attaques constatés parmi les entreprises ayant subi au moins une attaque. 5Sources : CESIN, OpinionWay).
• 79% Phishing ou spear-phishing
• 47% Arnaque au président
• 43% Exploitation d'une vulnérabilité
• 40% Tentatives de connexion
• 35% Ingénierie sociale
• 31% Acquisition de noms de domaines illégitimes
• 29% Exploitation d'un défaut de configuration
• 28% Attaque en déni de service

Avril 2020 : La cyberattaque par le rançongiciel Mespinoza/Pysa de la métropole Marseille – Aix en Provence a été qualifiée « d'inédite par son ampleur » et de « massive et généralisée ». 6 mois plus tard, les mêmes cyberattaquants font état de la fuite de 2 fichiers d'archives d'un volume d'environ de 20 Giga disponibles en download sur le site néo-zélandais d'hébergement de fichiers Mega. Des services et sociétés portuaires de Marseille et Port de Bouc sont impactés durant plusieurs semaines suite à cette attaque d'ampleur inhabituelle.

Septembre 2020 : Cyberattaque de CMA CGM, le quatrième armateur mondial dans le transport maritime par le ransomware Ragnar Locker actif depuis la fin 2019 et qui se base sur des vulnérabilités RDP (Remote Desktop Protocol) dans Windows de Microsoft. Le Groupe CMA CGM (hors CEVA Logistics) fait l'objet d'une cyberattaque sur des serveurs périphériques. Pour la première fois en France, une action judiciaire de cybercriminalité est réalisée conjointement par différents services d'enquête cyber de la gendarmerie nationale (Section de Recherches de Marseille – Section de Recherches de la gendarmerie maritime – Le C3N du PJGN de Pontoise – Négociateur GIGN) directement dans les locaux de l'armateur à Marseille.

Enfin, dernier exemple édifiant en matière de cybersécurité maritime, mentionnons le fournisseur israélien de solution de cyberdéfense, Naval Dome, qui a conduit une expérience sur un porte-conteneur de 260 m. Après avoir infecté l'ordinateur du capitaine du navire via un mail, une équipe de Naval Dome avait compromis le système de navigation, les radars et le système de gestion de la salle machines. Ils avaient pu ainsi dérouter le navire de sa route initiale et désactiver les moteurs. Un danger absolu sur les routes maritimes.

En tant que deuxième empire maritime mondial, la France a réagi en publiant un rapport du Secrétariat Général de la Mer (Matignon) en novembre 2018 qui s'engageait à prendre la mesure des enjeux liés à la cybersécurité dans le domaine maritime. Un an plus tard, un projet porté par la région Bretagne, affirme la volonté de beaucoup d'acteurs de la cybersécurité maritime, de s'engager réellement. Ainsi, la création d'un CERT- Maritime à Brest (initiative soutenue par le GYCAN[9]) est prochainement une réalité. L'ANSSI étant l'unique CERT en France, voilà qui apporterait une réponse

maritime complémentaire à tous les acteurs du monde maritime français qui en demandent la création. A l'instar de cette initiative, on ne peut pas omettre de mentionner celles qui existent également au sein d'autres régions de France (Normandie avec HAROPA Port du Havre – PACA – Pays de la Loire etc.) qui sont très dynamiques dans l'appréhension en matière de cybersécurité de ces phénomènes criminels numériques rapportés au domaine maritime et portuaire.

Mentionnons également que la Marine Nationale française a su réagir face aux diverses menaces maritimes en créant il y a déjà quatre ans (juin 2016), un MICA Center[10] au sein de la Préfecture Maritime de Brest. Le MICA Center est à ce jour, un acteur majeur dans la détection des criminalités organisées maritimes (cyber ou non).

Enfin, je ne peux omettre de mentionner l'unique service d'enquête judiciaire dévolu au monde de la mer, la cellule nationale de lutte contre la cybercriminalité maritime, CYBERGENDMAR. Placée au sein de la Section de Recherches de la gendarmerie maritime, ayant une compétence nationale, cette cellule réalise des enquêtes judiciaires ayant un caractère cyber auprès de tous les acteurs du monde maritime, à terre comme à bord des navires où elle peut se transporter.

Après ce long exposé d'un sujet qui me passionne depuis des années au travers des enquêtes que je conduis et des rencontres que j'y fait, je forme le souhait d'avoir pu vous éclairer sur une forme de cybercriminalité peu connue.

La prise de conscience de la menace cybercriminelle maritime est telle de la part des professionnels qu'aujourd'hui, l'ENSM[11], la Chaire Cyber Navale en collaboration avec IMT Atlantique, l'ENSTA Bretagne, et l'École navale, se sont associées afin de proposer un Mastère Spécialisé "cybersécurité des systèmes maritimes et portuaires" (début en septembre 2020).

L'innovation technologique dans le domaine des navires est permanente. Afin de réduire les risques liés à la navigation, comme ceux inhérents à l'activité économique, aujourd'hui déjà mais plus encore demain, nous verrons sur les mers du globe survenir l'avènement de l'ère des navires autonomes. Il ne s'agit déjà plus d'une utopie puisque des navires autonomes de taille modérée sont

déjà en fonction pour des transports simples. Demain, c'est la traversée d'un océan qui sera une réalité.[12]
Il s'agira donc d'être en capacité d'anticiper des cybers attaques menées contre ces navires autonomes. Le défi est de taille mais je ne doute pas de notre capacité à le relever. Les outils existent et se coordonnent déjà comme je vous l'ai exposé.
Je conclurai mon propos par les mots de Sénèque qui aujourd'hui autant qu'hier restent une vérité maritime : « L*orsqu'on ne sait pas vers quel port on navigue, aucun vent n'est le bon* ».

[1] lejournal.cnrs.fr
[2] fr.wiktionary.org
[3] Whatis.com / Wikipedia
[4] wikhydro.developpement-durable.gouv.fr
[5] Directive NIS
[6] Textes législatifs importants
[7] https://www.cesin.fr/fonds-documentaire-5eme-edition-du-barometre-annuel-du-cesin.html
[8] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/chiffres-et-tendances-des-cybermenaces-cybermalveillance-gouv-fr-devoile-son-premier-rapport-dactivite-2019#:~:text=Plus%20de%2090%20000%20victimes,de%20s%C3%A9curit%C3%A9%20qui%20les%20frappent.
[9] Groupement des Industries de Construction et Activités Navales
[10] Maritime Information Cooperation & Awareness Center
[11] Ecole Nationale Supérieure Maritime - Forme les officiers de la marine marchande
[12] En 2017, Rolls Royce imaginait déjà le navire autonome de 2020 Rolls Royce command

La cybersécurité : un enjeu incontournable pour le développement des drones maritimes et navires autonomes

Lieutenant de vaisseau OLIVIER JACQ,
doctorant, Chaire de Cyberdéfense des Systèmes Navals

Le développement des drones maritimes et navires autonomes est un sujet aujourd'hui régulièrement évoqué dans la presse maritime spécialisée. Les financements, annonces et essais se multiplient et augurent de réalisations industrielles et de déploiements opérationnels majeurs dans la décennie à venir. Les drones et les technologies associées (robotisation, intelligence artificielle, numérisation du domaine maritime) fascinent autant qu'ils suscitent, parfois, des craintes et des interrogations. D'une part, on peut en convenir : ces solutions ouvrent un nouveau champ des possibles, réduisent l'exposition de l'homme aux dangers inhérents du milieu maritime et concourent à améliorer drastiquement certaines capacités opérationnelles civiles et militaires. Mais par ailleurs, de nombreux défis demeurent avant un passage, serein, en phase d'industrialisation. Parmi ces défis, dans un contexte où le monde maritime et portuaire est régulièrement victime de cyberattaques, la cybersécurité ne peut être oubliée.

Le monde maritime a probablement été l'un des premiers à innover et à faire appel à la robotisation. Dans les domaines de l'exploration sous-marine, de l'*offshore*, de la guerre des mines, des EMR[1] ou encore des navires câbliers, les robots téléopérés (*Remote Operated Vehicles*, ROV) sont des alliés précieux de longue date. Ils concourent directement à réduire l'exposition de l'homme à des environnements dangereux, à améliorer l'autonomie et la sécurité des moyens engagés. Mais aujourd'hui, le développement des drones maritimes et navires autonomes va beaucoup plus loin : leur emploi est évoqué pour l'ensemble du spectre d'utilisation du domaine maritime et leur généralisation est une question de temps. Quelles sont les raisons pouvant expliquer cet engouement ?

Les drones et navires autonomes : des apports (in)discutables

Une des premières vertus associées aux drones et navires autonomes serait de réduire le nombre d'accidents en mer, pour lesquels les enquêtes soulignent régulièrement le facteur humain comme cause première ou concourante d'incident ou d'accident. La fatigue, les erreurs de jugement, les négligences, le manque de formation et d'entraînement sont ainsi souvent pointés du doigt[2]. La généralisation de l'emploi des drones maritimes et navires autonomes permettrait donc de limiter l'occurrence et la sévérité de ce type d'évènements.

La réduction des coûts est également une des raisons mises en avant pour l'emploi des drones et navires autonomes. Dans un contexte très concurrentiel, si on élude l'investissement initial et les coûts de fonctionnement et d'exploitation des centres de contrôle à distance, le coût horaire, de maintenance et, *in fine*, la rentabilité d'un drone ou d'un navire autonome sont des arguments de poids pour les constructeurs et exploitants.

Au-delà de l'aspect économique, l'absence d'équipage fait aussi subir un régime drastique aux navires autonomes : la passerelle, les zones de repos, cabines, cuisines, certains espaces de stockage et cuves disparaissent. L'équipage ne produit plus de déchets, ne consomme pas d'eau, la consommation électrique à bord est globalement diminuée, la consommation en carburant réduite de moitié[3] et les émissions de CO2 optimisées : l'argument environnemental n'est donc pas négligeable, d'autant plus que la diminution du tonnage permettra l'emport de batteries pour permettre une propulsion électrique partielle ou totale.

Ces arguments peuvent expliquer que les drones maritimes de surface et sous-marins sont en plein essor dans le monde maritime civil. Les expérimentations dans des domaines novateurs pour des navires autonomes (transport de passagers et de voitures, remorquage) se multiplient. En Europe, on pourra notamment évoquer la démonstration de faisabilité récente de SeaOwl avec le VN Rebel, mais aussi les réalisations Seakit, DriX, Falco/SVAN, AI Captain, sans oublier le projet du Yara Birkeland, qui sera sans précédent en termes de tonnage. A terre, le nombre de centres de

contrôle à distance de drones augmente et plusieurs centres devraient voir le jour à Brest. Le développement de ces nouveaux équipements se heurte cependant à une réglementation parfois lacunaire ou non adaptée. En conséquence, les essais actuels se déroulent essentiellement dans les eaux nationales avec, en Europe, des démonstrations récentes dans les pays nordiques (Danemark, Norvège, Finlande), mais aussi en France. Des travaux importants sont également menés pour concilier sûreté, sécurité, environnement et développement industriel et opérationnel. Dans le cadre de son comité de sécurité maritime et conformément à son plan stratégique 2018-2023, l'Organisation Maritime Internationale (OMI) mène ainsi les travaux réglementaires nécessaires pour permettre l'emploi des navires autonomes (MASS[4]) dans les eaux internationales, en veillant notamment au respect des règles internationales pour la prévention des abordages (COLREG) et pour la sauvegarde de la vie en mer (SOLAS). En France, le Cluster Maritime Français (CMF) a également publié récemment un « Guide de bonnes pratiques relatives aux drones maritimes », qui émet de nombreuses recommandations sur l'emploi des drones et navires autonomes et qui évoque les questions de cybersécurité[5]. Les travaux de certification et d'assurance des drones et navires autonomes sont également déjà réalisés ou en cours.

Classification des MASS par l'OMI en fonction de leur connectivité et de la présence de marins à bord[6] :
1er degré - Navire avec des processus automatisés et une capacité de décision : des marins sont présents à bord pour opérer et contrôle les systèmes et fonctions du navire. Certaines opérations peuvent être automatisées et parfois non supervisées, mais les marins à bord sont parés à reprendre la main.
2ème degré - Navire contrôlé à distance avec des marins à bord : le navire est contrôlé et opéré à partir d'un autre emplacement. Des marins sont présents à bord pour prendre la main et opérer les systèmes et fonctions du navire.
3ème degré - Le navire est contrôlé à distance, il n'y a pas de marin à bord.
4ème degré - Navire totalement autonome : le système du navire est capable de prendre les décisions et de déterminer ses actions par lui-même.

Au niveau militaire, de nombreuses marines de premier rang sautent le pas et s'engagent résolument pour démultiplier leurs capacités opérationnelles par l'emploi des drones. D'ici 10 ans, la plupart d'entre elles disposeront de

drones aériens, sous-marins et de surface déployables en mer sur les théâtres d'opération et en protection des approches du territoire national. Les tailles (nanodrones, microdrones, minidrones et drones) et domaines d'emploi (aérien, surface, sous-marin) multiplient les possibilités d'emploi des drones maritimes. Parmi les premiers cas d'usage figurent les planeurs sous-marins pour la surveillance de l'environnement et le renseignement, les drones dédiés à la guerre des mines, et les drones embarqués à bord de navires porteurs : la multiplicité des capteurs embarqués, les missions multi-drones et l'autonomie offerte permettent d'étendre la couverture de détection et facilitent l'acquisition de renseignement dans des zones complexes ou dangereuses.

Des cibles de choix ?

Lorsqu'on parle de cybersécurité, la tendance assez généralisée consiste à n'évoquer que l'attaque volontaire. Or, par conception, le drone maritime et le navire autonome sont des systèmes de systèmes numériques complexes : il serait donc inapproprié de ne pas prendre en compte le risque de défaillance d'un sous-système, voire de l'ensemble du système. Pour les drones et navires les plus évolués, la disparition de la présence humaine à bord n'est pas neutre : si l'homme est parfois perçu comme un facteur de risque potentiel en termes de sécurité nautique (ou informatique !), le marin joue pourtant un rôle essentiel pour la maintenance des systèmes embarqués. En cas de panne ou d'avarie, la maintenance à distance des systèmes mécaniques, électroniques et informatiques à bord du navire autonome atteindra rapidement ses limites. La disponibilité des drones maritimes et navires autonomes s'appuiera donc fortement sur la redondance des équipements à bord. Cette redondance, indispensable, augmente aussi la surface d'attaque potentielle du navire.

Le drone maritime et le navire autonome, qu'ils soient civils ou militaires, présentent de multiples intérêts pour les attaquants. Leur coût et l'avantage opérationnel qu'ils apportent peuvent en faire des cibles de choix pour une demande de rançon, une capture physique ou à des fins d'espionnage industriel. Les données qu'ils peuvent contenir (détail de la mission attribuée, données capturées) sont également de valeur. L'attaque dans un but de destruction, de sabotage et de détournement de la mission initiale doit également être prise en compte : retourner un drone contre le navire qui l'a mis en œuvre n'est pas un scénario réservé à Hollywood, mais se doit de

figurer dans une analyse de risques. Les impacts sur la réputation du concepteur, de l'opérateur ou du pays du drone attaqué ne sont pas à négliger. Enfin, le centre de contrôle à terre est un point névralgique : concourant directement à la planification, à la réalisation et à l'analyse des missions des engins autonomes, une cyberattaque le visant pourrait avoir des impacts conséquents sur la flotte qu'il contrôle.

It's not a bug, it's a feature !

Les concepteurs de drones maritime et navires autonomes doivent faire face à de nombreux défis en termes de cybersécurité : les vulnérabilités liées à l'*Automatic Identification System* (AIS) et à certains systèmes de Géolocalisation et Navigation par un Système de Satellite (GNSS) ont été démontrées par les chercheurs depuis de nombreuses années. Les cas de leurrage AIS et de leurrage et de brouillage GPS sont fréquemment remontés par les marins de par le monde. Certains systèmes de communication par satellite ont aussi récemment montré leurs faiblesses, permettant l'interception de données avec des systèmes coûtant tout au plus une centaine d'euros. Enfin, depuis les années 2010, les incidents et cyberattaques sur les systèmes de contrôle industriels sont également largement documentés.

Or, le drone maritime et le navire autonome reposent justement sur l'AIS, les GNSS, les moyens de télécommunication par satellite pour fonctionner. Le navire autonome, lui, est automatisé au maximum et, en plus des systèmes qu'il partage avec le drone maritime, dispose de systèmes industriels encore plus nombreux pour commander la propulsion, la production d'électricité, etc. Drones maritimes et navires autonomes mettent donc en œuvre, par conception, des systèmes dont les vulnérabilités sont connues et, pour certaines, à la portée d'un attaquant non étatique de niveau moyen. Comment réagissent ces engins en cas de leurrage, de brouillage AIS ou GNSS ou de perte du lien satellite de télécommande et de supervision ?

Enfin, au-delà des systèmes évoqués ci-dessus, drones maritimes et navires autonomes embarquent d'autres éléments indispensables à leurs missions. Tout d'abord, des capteurs supplémentaires y sont installés pour compenser l'absence d'être humain : au classique radar on ajoute ainsi de nombreuses caméras dans différents spectres, capteurs environnementaux et d'attitude.

Mais, surtout, au cœur du drone et du navire autonome se trouve un nouveau système : son « intelligence ». Au-delà de l'acronyme IA, largement dévoyé, une certitude : le drone et le navire ont, localement, recours à des outils de réalisation de mission et de prise de décision. En se basant sur des données en entrée (mission, capteurs), le drone est capable de disposer d'une « intelligence de la situation » (*situational awareness*) et évolue en fonction pour accomplir sa mission en tenant compte de l'ensemble des paramètres. Ce recours à l'algorithmie et aux données, particulièrement puissant, nécessite cependant beaucoup de soin dans sa conception et sa réalisation : les algorithmes doivent avoir été rigoureusement analysés et testés pour apporter la preuve formelle qu'ils sont sûrs[7]. Il ne doit pas exister de cas non prévu ou non testé et le drone ou navire doivent toujours pouvoir se mettre dans une position de sécurité et d'attente en cas de danger ou de perte de télécommande, par exemple. Enfin, s'il parvient à obtenir le modèle de fonctionnement du drone, l'attaquant dispose d'un avantage tactique réel : il peut anticiper la réaction de l'engin face à une situation donnée et la tourner à son avantage pour parvenir à ses fins.

Quelles responsabilités en cas d'évènement ?

Le cas de l'attaque cyber est dorénavant souvent évoqué pour les drones et navires autonomes : les constructeurs en sont conscients et, en conception, réduisent les risques du mieux qu'ils peuvent. Mais ils font face à plusieurs défis. En premier lieu, comme nous l'avons déjà évoqué, certains protocoles et équipements utilisés sont vulnérables par conception et difficiles à sécuriser : il est ainsi difficile d'apporter une preuve formelle de la sécurité de l'AIS, du GNSS ou de certains liens satellites. Ensuite, la multiplicité, dans la provenance et le fonctionnement, des composants d'un drone ou d'un navire autonome complexifie la sécurité de l'ensemble. Ainsi, la gestion coordonnée et *in time* de l'application des correctifs (maintien en conditions de sécurité) devient particulièrement complexe. En cas de cyberattaque, la détection sur un ou plusieurs systèmes distants, l'analyse et la réaction en l'absence d'être humain à bord sont particulièrement ardues. Enfin, qui sera jugé responsable en cas de dysfonctionnement du drone ou du navire suite à une attaque ou un dysfonctionnement ayant entraîné un accident ? Le concepteur d'ensemble, les fournisseurs du matériel ou du logiciel, l'exploitant, le centre de contrôle à terre, voire, l'algorithme[8]?!

La route tracée des drones maritimes et navires autonomes vers la cybersécurité

Les mondes de la recherche et de l'industrie, les instances régulatrices et de certification ont donc encore de nombreux travaux à mener pour aboutir à des solutions sûres. Si l'homme sera peut-être un jour remplacé par l'intelligence présente dans ces engins, son expertise et son expérience seront essentielles en phase de conception et d'exploitation. Au-delà des recommandations, le régulateur devra fixer de hauts niveaux d'exigences en cybersécurité, probablement via des démarches d'homologation et de certification comprenant des audits et tests d'intrusion, avec une attention particulière sur les modes dégradés. Pour les industriels et chantiers navals, le drone maritime et le navire autonome sécurisés par défaut devront être un avantage concurrentiel. La maîtrise du cycle de ces engins ne devra pas être négligée : comme un navire de surface, leur durée de vie sera particulièrement longue. Enfin, la surveillance cyber temps-réel de l'intégrité des drones maritimes et navires autonomes sera une mission essentielle pour les centres de contrôle.

[1] Énergies Marines Renouvelables
[2] Allianz Global Corporate & Specialty, *Safety and shipping review* 2018
[3] Rødseth, Ørnulf Jan and Burmeister, Hans Christopher, *Developments toward the unmanned ship*
[4] *Maritime Autonomous Surface Ship*
[5] https://www.cluster-maritime.fr/wp-content/uploads/2020/06/CMF_guide_drones_juin2020.pdf
[6] http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-100th-session.aspx
[7] Rødseth, Ørnulf Jan and Burmeister, Hans Christopher, *Risk Assessment for and Unmanned Merchant Ship*
[8] L'algorithme jouerait en effet le rôle du capitaine à bord du navire : il est donc censé endosser l'ensemble des responsabilités initiales en cas d'incident !

Automatiser la cybersécurité, un enjeu d'innovation crucial dans le domaine maritime

WILLIAM LECAT
Directeur de programme Grand Défi automatisation de la cybersécurité,
Secrétariat Général pour l'Investissement

Le domaine maritime présente en France des enjeux de souveraineté et économiques considérables, que ce soit au niveau de la marine nationale ou de la marine marchande. En effet, le pays dispose du deuxième plus grand espace maritime mondial avec 11 millions de km², principalement en Outre-mer, derrière les Etats-Unis. L'économie y est naturellement très active avec plus de 354 000 emplois directs pour une valeur de production de plus de 90Mds€ annuelle. Au niveau mondial, l'activité est en croissance également. L'OCDE prédit que le poids du maritime dans l'économie mondiale devrait doubler d'ici 2030 pour atteindre les $3 000Mds annuels sachant que le transport de marchandise du commerce mondial repose à 90% sur le transport maritime.
(Source : https://www.cluster-maritime.fr/economie_maritime/)

Comme dans beaucoup de domaines, la numérisation s'y accélère pour atteindre un grand nombre d'aspects de ce secteur, que ce soient au niveau des navires et de leurs différents systèmes, des infrastructures portuaires et même des cargaisons. Les systèmes sont particulièrement complexes, mêlant systèmes d'information, systèmes industriels avec des notions de temps réel, embarqué avec des contraintes de place et de ressources (consommation et capacité de calcul) et mobilité avec des problématiques de communication limitée (bande passante, latence, disponibilité, etc.). Le tout étant bien sûr de plus en plus interconnecté par des réseaux IP (Internet Protocol), exposant ainsi le cœur des systèmes historiquement isolés et très spécifiques à toutes les menaces classiquement présentes sur Internet.

Il en découle naturellement de plus en plus d'attaques, en particulier sur les infrastructures portuaires qui sont, de manière inquiétante, la cible de «

ransomware » à une fréquence grandissante. Depuis 2017 et l'expérience de Naval Dome sur porte conteneur, l'exposition des navires eux-mêmes aux cyberattaques est démontrée. Avec en perspective une estimation de plus 90 000 navires commerciaux en circulation, la menace est considérable. Cependant, les contraintes de l'embarqué et de la mobilité, par exemple, perturbent les modèles standards de protection et de défense contre les attaques. Il est d'abord souvent difficile de remonter toutes les informations en temps réel vers un « Security Operation Center » (SOC) distant et centralisé du fait de bandes passantes souvent limitées depuis les navires. Il est ensuite impossible d'embarquer un SOC local sur chacun des bâtiments pour des raisons évidentes de place et de passage à l'échelle. De plus, les systèmes industriels critiques des bateaux (par exemple de propulsion ou de navigation) induisent souvent des contraintes de temps réel nécessitant un délai très court entre un incident cyber, sa détection et sa remédiation pour éviter des conséquences possiblement dramatiques.

Ces aspects militent fortement pour deux notions complémentaires aux modèles actuels : une capacité de détection locale, c'est-à-dire au plus proche des équipements supervisés, et une orientation vers une remédiation simplifiée voire à terme automatique pour garantir la résilience nécessaire à ces systèmes face aux attaques qui ne manqueront pas de survenir. En se focalisant sur les navires, on peut décrire les interactions avec différents autres systèmes maritimes, c'est-à-dire les autres navires, les infrastructures aux sol du constructeur et de l'armateur, les infrastructures portuaires et parfois les cargaisons, sachant que le navire peut être dans deux configurations totalement distinctes correspondant à deux situation très différentes : à quai avec une connectivité potentiellement plus (parfois trop ?) importante permettant toute sortes de maintenances et en mer avec une relative isolation et donc la nécessité d'un niveau d'autonomie plus élevé.

Comme souvent dans des domaines en cours de numérisation rapide, la première difficulté du point de vue de la sécurité est de s'interfacer avec les anciennes générations d'équipements qui ne prennent que peu en compte la sécurité, d'autant plus quand, comme ici, les cycles de renouvellement des matériels peuvent être très longs. Néanmoins, le design de nouvelles architectures pertinentes permet d'incarner l'objectif à atteindre. Historiquement, les concepts de protection cyber ont progressivement évolué

de la défense périmétrique (confiance à l'intérieur du périmètre du système avec une barrière le protégeant) vers une défense en profondeur (consistant schématiquement à multiplier les périmètres de manière concentrique) ensuite complétés par la notion, à la mode actuellement, de « Zero Trust ». Cette dernière notion est relativement récente dans ses implémentations (bien que le concept ait plus de 10 ans) et est principalement appliqués aux systèmes d'information « classiques ». Il serait particulièrement intéressant de l'appliquer au domaine maritime sur les nouveaux systèmes et dans leur intégration avec les anciens malgré les challenges, en particulier au niveau des systèmes industriels, que cela représente. En effet, les grands principes semblent particulièrement adaptés. Il s'agit d'appliquer une séparation des réseaux particulièrement fine (micro-segmentation), ce qui est essentiel sur un navire comprenant des dizaines de systèmes différents. Ensuite, le principe des privilèges minimaux pour les tâches à effectuer (et variables en fonction de l'état de menace) complète le modèle pour minimiser les risques de compromission et de mouvement latéral. Pour être mise en place, cette approche passe typiquement par une gestion fine des identités des utilisateurs et des services accessibles. Néanmoins, dans un système industriel s'appuyant massivement sur l'automatisme, il est important d'étendre la notion d'identité pour intégrer « l'identité » des processus d'automatisme. En effet, si un processus automatique a besoin d'accéder à un service pour réaliser sa mission, le modèle du « Zero Trust » peut être étendu en associant l'identité du processus à une capacité de garantie de son intégrité (i.e. il s'agit du bon processus, non altéré). Ainsi, les « utilisateurs » (personnes ou processus d'automatisme) se voient ainsi autorisés l'accès minimal nécessaire en fonction de la tâche à réaliser, du niveau de confiance dans l'authentification (mot de passe, multi facteurs, intégrité du processus, etc.), du niveau de santé de l'équipement support à l'utilisateur (enrôlé ou non dans un système de management des équipements, niveau de mises à jour, compromission ou non suspectée de l'équipement, etc.) et du niveau du service accédé (niveau de criticité, niveau de mises à jour, etc.). Cela passe classiquement par un système de gestion des identités et de l'authentification et un système de management des équipements permettant une supervision globale des équipements, des services et des utilisateurs. Un utilisateur peut donc avoir différents niveaux d'accès (total, virtualisé ou refusé par exemple) en fonction du contexte (de connexion, des équipements et du service visé). Pour être pertinent, un recourt massif à la « Cyber Threat Intelligence » (CTI) est

essentiel pour apporter une contextualisation aux différentes configurations observées. L'intérêt d'un modèle comme celui-là réside également dans la capacité à le mettre en place de manière incrémentale (gestion des identités, puis des équipements, puis des services, etc.) tout en prenant en compte l'existant avec un niveau d'intégration variable (impossibilité de superviser certains équipement anciens, accès restreint à des équipements obsolètes potentiellement vulnérable mais essentiels, etc.).

Ce type d'approche est totalement complémentaire d'une analyse de risque préalable, voire continue qui passe par la cartographie en temps réel des systèmes (et l'analyse de leur criticité), la cartographie des interactions (en particulier sur les processus industriels) pour permettre la micro-segmentation active (i.e. imposée par les éléments actifs de réseau) ou passive (i.e. levant des alertes en cas d'infraction). Cela doit permettre d'avoir une vision à jour du système au niveau des équipements, de leurs interactions et de leurs vulnérabilités tout en la contextualisant avec les éléments de CTI (de haut niveau avec par exemple les campagnes d'attaque en cours dans le secteurs économique ou géographique ; plus bas niveau avec la criticité des vulnérabilités et les marqueurs de détection).

Ces focus sur la cartographie et la CTI doivent permettre les mécanismes attendus de détection basés sur les marqueurs (détection de codes ou de flux malveillants) mais également ceux basés sur la détection d'anomalies. Par exemple, grâce à des modèles d'apprentissage machine validés par les connaissances métier, on peut espérer détecter les comportements anormaux en particulier sur des systèmes industriels fortement encadrés par des processus clairement définis. Ces détections, contextualisées avec l'analyse de risque permettent donc d'envisager la priorité et le type de remédiation à appliquer. En fonction, de la criticité de la fonction industrielle touchée, on peut par exemple tolérer la corruption et simplement l'isoler (quand il s'agit d'une fonction annexe) ou à l'opposer opérer une levée de doute (à terme automatiquement) car les faux positifs ne peuvent être tolérés, la restauration étant particulièrement couteuse. Se dégage alors deux notions déjà très classiques de résilience (correspondant plus à de la continuité d'activité malgré l'incident, i.e. un PCA) et de remédiation (plus orientée sur la reprise de l'activité après une réponse à l'incident pour restaurer l'état normal, i.e. un PRA). Les deux aspects peuvent très certainement coexister sur un système

en fonction des spécificités et des criticités des différents processus.
En complément de tous ces dispositifs pouvant être mis en œuvre, une démarche de collecte massive de données sur les systèmes maritimes est essentielle. Que ce soit des journaux d'événements, des traces réseaux, l'historique des mises à jour ou tout autre élément permettant de modéliser le bon ou le mauvais fonctionnement de ces systèmes, ces données sont aujourd'hui les éléments nécessaires au design des futurs algorithmes avancés de sécurité (pas uniquement cyber) et seront demain véritablement le carburant permettant de faire tourner ces mêmes algorithmes devenus essentiels au bon fonctionnement des systèmes. Il est urgent de mettre ne place les dispositifs pour capter, prétraiter et stocker de manière sécurisée ces éléments qui contiennent une richesse informationnelle immense et qui seront très vite sources de création de valeur.

Quoi qu'il en soit, le constat reste que sur un navire, le nombre de personnels spécialisés en cybersécurité reste très limité. Il est donc essentiel à la fois de sensibiliser l'équipage aux problématiques pour limiter les risques de compromission et surtout lui permettre de réagir adéquatement mais aussi d'automatiser au maximum les processus cyber pour qu'ils puissent être opérés sans compétence spécifique à bord.

C'est sur cet aspect de l'automatisation que le Grand Défi Cyber met l'accent au travers de développements technologiques et de soutien à l'innovation. Dans son premier axe vertical, la feuille de route du Grand Défi insiste sur l'impact que les nouveaux usages ont sur les réseaux, les rendant extrêmement dynamique. L'importance de la cartographie identifiée depuis longtemps n'en devient que plus critique. L'un des objectifs de cet axe est donc de favoriser l'émergence d'offres et de technologies permettant d'assurer cette brique fonctionnelle fondamentale sur laquelle se basera tout le reste de l'automatisation dans les réseaux. La cartographie se décline sous plusieurs formes qui ont toutes leur importance : équipements, services et autres logiciels installés, les interactions, etc. L'objectif suivant sera d'aboutir à des capacités d'analyse de risque dynamique permettant dans l'idéal d'avoir une vue contextualisée sur les risques et les mesures prises avec un focus particulier sur la possibilité de mesurer les impacts (en particulier financiers) et donc les retours sur investissements potentiels. En parallèle, le développement de possibilités de détecter et d'intervenir localement sur les équipements (en

particulier ceux embarqués et critiques) permettra de favoriser le tournant vers une remédiation automatisée grâce à l'orchestration des différentes solutions de sécurité. La première cible sera de démontrer la possibilité d'automatiser la levée de doute qui prend un temps trop important aux experts. Enfin, toutes ces capacités reposent bien évidemment sur une « Cyber threat Intelligence » de qualité et de confiance. En France, nous avons structurellement peu d'entités qui possède à la fois la capacité, de par leur positionnement, à capter de grandes quantités de données représentatives et la capacité à les valoriser sous l'angle cyber. Il sera très important de rapprocher ces différentes typologies d'acteurs autour de projets innovants dans le but de faire émerger une offre de CTI française voire européenne. De plus, un deuxième axe, dédié aux objets connectés, mettra l'accent sur les technologies permettant la résilience cyber de ces nouveaux équipements bientôt omniprésents. Avec en tête la convergence des différents domaines (IT, OT, IoT, etc.) vers une technologie unifiée autour de l'IP (Internet Protocol), le Grand Défi cyber vise à aider le développement parfois risqué (financièrement ou techniquement) de technologies de rupture et à soutenir l'émergence de futurs acteurs majeurs.

Réflexions juridiques autour de l'assurance des cyberisques maritimes

OLIVIER LASMOLES
Professeur associé de droit, EM Normandie

« Aux pirates en mer se sont substitués les hackers. Et ce dernier espère tout autant que leurs homologues voler et détourné de leur cadre légal des informations, des données, et des infrastructures, afin d'en faire un usage frauduleux »[1].

Le transport maritime, qui représente plus de 90% du commerce international, voit ses navires se transformer en objets connectés, intégrant sans cesse plus de technologie et de systèmes automatisés. L'utilisation de ces technologies par les compagnies maritimes et les acteurs portuaires offre de nombreux avantages : réduction des effectifs, augmentation de l'efficacité des opérateurs, interchangeabilité des équipements... Depuis quelques années, cependant, nous assistons à une recrudescence des cyberattaques dans le milieu maritimo-portuaire.

La complexité du monde cyber risque fait que les compagnies maritimes ainsi que les acteurs portuaires, dans un souci de maîtrise et de capacité technologique, optent pour un transfert de ce risque vers le marché de l'assurance. Mais avant d'aller plus loin, définissons le cyberisque. Les définitions étant multiples, nous en proposerons deux : la première, données par les assureurs, le définit comme « tout risque de perte financière, d'interruption des activités où d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologie de la formation »[2]. L'Organisation de coopération et de développement économiques (OCDE) dans sa recommandation (VII.1) de 2015 définit le cyber risque comme « une catégorie de risques liée à l'utilisation, au développement et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit »[3]. L'absence de définition faisant l'unanimité démontre la méconnaissance du

cyberisque par l'ensemble des acteurs. Cette méconnaissance influence-t-elle sa prise en charge par les assureurs ? Quelle stratégie assurantielle l'industrie de l'assurance doit-elle adopter ?

Les difficultés rencontrées par les acteurs maritimo-portuaires et les assureurs tiennent aux spécificités de la cybersécurité maritime (I) et aux défis que ces risques leur posent (II).

Les spécificités de la cybersécurité maritime

Le monde maritime et industrialo-portuaire a tardivement pris conscience de la menace que représentent les cyberisques. Cela s'explique, notamment, par le caractère systémique de ce type de risque (A) qu'il est peu aisé d'appréhender. Cependant, une fois cette prise de conscience actée, une réglementation *ad hoc* (B) a vu le jour permettant de définir les gestes barrières propices au développement d'une hygiène de la cybersécurité.

Un risque systémique tardivement perçu

Dans son rapport sur l'évolution des risques du système financier français, la Banque de France a mis en évidence que la digitalisation renforce à la fois « le risque d'un incident cyber et son impact potentiel tant pour les institutions et les infrastructures financières immédiatement touché que pour le système financier dans son ensemble » ; avant de conclure que « le risque cyber n'est plus un risque opérationnel idiosyncratique, il devient potentiellement systémique »[4]. Le risque systémique pouvant être appréhendé comme « un risque de dégradation brutale de la stabilité financière, provoqué par une rupture dans le fonctionnement des services financiers, et répercuté sur l'économie réelle »[5]. Le cyber risque serait donc « un risque systémique qui se dessine au-delà des frontières géographiques mais dont les modes de propagation et d'agrégation sont loin d'être maîtrisés »[6].

Une cyberattaque peut toucher plusieurs acteurs maritimes et portuaires, provoquant des demandes d'indemnisation à grande échelle. En effet, les acteurs concernés utilisent les mêmes plateformes portuaires, les mêmes *Port Community System* ; ce qui peut faciliter la propagation d'un virus.

Malgré ces menaces, il faudra attendre 2011 pour que le Bureau Maritime

International (BMI) tire la sonnette d'alarme et que l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ne publie un rapport sur la sécurité en matière maritime. Le rapport soulignait le faible niveau de protection du monde maritimo-portuaire face à d'éventuelles cyberattaques.

La plus importante cyberattaque ayant touché le monde maritime reste celle de Notpetya en juin 2017, touchant le groupe AP Moller-Maersk et occasionnant des pertes de plus de 300 millions de dollars. La dernière en date et celle d'avril 2020 visant le centre de données du groupe MSC à Genève, qui a contraint le groupe à restreindre l'accès à son site internet pendant plusieurs jours. Si les cibles des cyberattaques sont avant tout les systèmes terrestres des compagnies maritimes et du monde portuaire, la sophistication des outils employés permet, dorénavant, de cibler les navires en mer, pouvant aller jusqu'à leur détournement.
L'impact de ces attaques ne se limite plus à la gestion de la perte ou du vol de données. Les atteintes à la propriété, à la réputation, ainsi qu'aux coûts liés à la perte d'exploitation sont des préoccupations croissantes. Selon une étude de l'institut Ponemon[7], la perte d'information est la conséquence la plus coûteuse d'un incident cyber, représentant 39% des coûts ; suivi de la perte d'exploitation avec 36 % des cours. La perte de revenus étant évaluée à 20%.

Une réglementation *ad hoc*
La couverture de risque nécessite un encadrement juridique permettant à l'assuré de connaître ses obligations et à l'assureur de l'accompagner dans le maquis des textes nationaux, communautaires et internationaux.

La France a été précurseur en matière de lutte contre les cyberisques. En effet, le Livre blanc sur la Défense et la Sécurité nationale de 2008 avait souligné la nécessité d'élaborer une doctrine en la matière. C'est également le Livre blanc de 2008 qui avait acté la nécessité de créer une agence chargée de la sécurité des systèmes d'information. Le livre blanc de 2013 avait fixé la doctrine officielle en matière de cybersécurité en installant l'appareil législatif des Opérateurs d'Importance Vitale (OIV) et en créant la notion de Systèmes d'Information d'Importance Vitale (SIIV). Les secteurs d'activités d'importance vitale sont aujourd'hui au nombre de douze ; dont les

transports et l'industrie depuis le 1er octobre 2016.

Tenant compte des spécificités du transport maritime, la direction générale des Affaires Maritimes a publié en septembre 2016 un guide sur la cybersécurité et la protection des navires. Cette publication a été suivie en octobre 2016 de celle des Affaires Maritimes et de l'ANSSI à travers un guide des bonnes pratiques de sécurité informatique à bord des navires. Enfin, en janvier 2017, les Affaires Maritimes publié un guide concernant le renforcement de la protection des systèmes industriels des navires face aux cyber risques.

L'Union européenne (UE) a perçu, très tôt, les enjeux liés à la cybersécurité. C'est ainsi qu'elle a créé l'ENISA dès 2004. Mais la pierre angulaire de la politique de l'UE en la matière reste la directive du 6 juillet 2016 sur la sécurité des réseaux et des systèmes d'information connu sous l'appellation « directive NIS ». Elle comporte quatre grands axes : les États membres doivent se doter d'autorités nationales compétentes en matière de cybersécurité ; la directive prévoit l'établissement d'un cadre de coopération volontaire entre les États membres de l'UE ; elle crée une nouvelle catégorie d'opérateurs au travers des Opérateurs de Services Essentiels (OSE) ; enfin, elle prévoit des règles européennes communes en matière de cybersécurité des prestataires de services numériques.

A l'échelle internationale, le premier, et unique, traité touchant à la cybersécurité est la convention de Budapest sur la cybercriminalité du 23 novembre 2001.

La prise de conscience des cyberisques maritimes au niveau international a conduit l'organisation maritime internationale (OMI) ainsi que des acteurs du secteur privé à réagir. Avant 2016, il était possible de s'appuyer sur les deux seuls textes traitant de la cybersécurité maritime. Le premier est le code ISPS, traitant de la lutte contre le terrorisme, qui impose aux transporteurs maritimes d'appliquer les mesures de protection physique des systèmes d'information du navire. Le second texte est le Code ISM, *International Safety Management*, qui impose aux transporteurs maritimes de rédiger une politique compagnie sur les systèmes d'information du navire et de contrôler les échanges des systèmes d'information du navire. Mais ces textes, malgré

leur qualité, étaient clairement inadaptés aux cyberisques maritimes actuels. C'est pourquoi, l'OMI a publié, en 2017, des recommandations sur la gestion des cyberisques maritimes[8]. La même année, l'OMI a adopté une résolution sur la gestion des cyberisques maritimes dans le cadre des systèmes de gestion de la sécurité[9]. Elle reconnaît dans l'alinéa premier de la résolution, qu'il est « urgent de sensibiliser aux menaces et aux vulnérabilités en matière de cyberisques afin de renforcer la sécurité et la sûreté des transports maritimes pour qu'ils aient une résilience opérationnelle face aux cyber risques ». L'OMI encourage les administrations nationales à s'assurer que les cyberisques maritimes sont incorporés dans les systèmes de gestion de la sécurité. Cette recommandation doit être appliquée au plus tard à la date de la première vérification annuelle du document de conformité délivré à la compagnie après le 1er janvier 2022.

Les travaux de l'OMI ont été complétés par ceux d'associations maritimes internationales. Dans un manuel publié en 2019[10], le *Baltic and International Maritime Council* (BIMCO), en association avec l'*International Chamber of Shipping* (ISC), démontre que le risque cyber ne peut plus être ignoré. Les rédacteurs de ce manuel estiment que « la création d'une culture et d'une conscience cybernétique, centrée sur les mesures de protection, de prévention et de formation est cruciale »[11]. Pour cela, le manuel identifie les risques menaçant les vecteurs d'attaque les plus courants ; avant d'approfondir la protection et la prévention. Il est, en outre, demandé aux compagnies d'élaborer un plan d'intervention en cas d'attaque.

D'autres études fournissent des recommandations sur la gestion des cyberisques. L'une d'entre elles souligne que ces risques nécessitent d'« identifier les rôles et responsables des utilisateurs, et personnels clés et des cadres à terre comme en mer ; recenser les systèmes, les actifs, les données et les capacités qui pourraient menacer d'exploitation et la sécurité des navires en cas de perturbations ; mettre en place des mesures techniques pour protéger contre un cyber incident et assurer la continuité de l'exploitation »[12].

Outre l'intérêt opérationnel de ces recommandations, celles-ci permettront aux assureurs d'avoir un référentiel en matière de gestion des risques sur lequel elles pourront s'appuyer lorsqu'il s'agira d'évaluer la politique cyber des compagnies maritimes. De manière générale, « les normes sont des exigences

et des points de contrôle permettant aux entreprises de décliner les exigences réglementaires et les exigences de sécurité, tout en rassurant les interlocuteurs externes et la direction »[13].

La nécessité de la prise en compte des cyberisques par les assureurs apparaît, donc, comme une évidence. Ils devront, cependant, relever de nombreux défis, de natures différentes.

Les défis posés aux assureurs maritimes

Ces défis ont, tout d'abord, pour origine la difficile appréhension des cyberisques (A) due, notamment, à leur quantification complexe. La digitalisation croissante des navires (B) est un autre défi, a fortiori dans un monde cybermaritime sans frontières, à double titre.

La difficile appréhension des cyberisques
Malgré la recrudescence des attaques cyber dans le monde maritime ces dernières années, peu de données ont été collectées quant à leurs origines, leurs volumes... Cette absence de données ne facilite pas la tâche des assureurs maritimes en matière de tarification. Les nombreuses incertitudes entourant ces risques incitent les assureurs à une prudence extrême. Selon une étude du gouvernement britannique et de la compagnie d'assurance Marsh, le coût médian de couverture pour un contrat couvrant les cyber risques et trois à six fois plus élevé que pour des contrats de type responsabilité civile ou dommages[14]. Plusieurs critères permettent de différencier les risques : le secteur d'activité ; des indicateurs clés tels que le chiffre d'affaires ; la capacité à traiter, stocker et sécuriser des données à caractère personnel ; le niveau de sécurité des systèmes d'information et de conformité aux normes. Or, les franchises, les limites de sécurité peuvent permettre aux compagnies d'assurance d'ajuster leurs tarifs. Dès lors, le niveau de prime, au regard de l'appréciation de la couverture, est souvent cité comme l'un des obstacles importants à la souscription d'assurances cyber.

Une autre question, épineuse, se pose aux assureurs : celle de la modélisation du cyberisque. Celle-ci « mesure précisément l'écart entre les pratiques d'une société et ce qu'on peut considérer comme les meilleures pratiques ». Dans le rapport Hiscox 2019[15], on apprend que seul 10% des entreprises, tous

secteurs confondus, ont obtenu la mention « expert » dans la capacité de gestion de leurs risques cyber. Plus de 74 % n'ont obtenu la mention « expert » dans aucun des domaines (stratégie, contrôle, ressources, technologies et procédure) et 16% sont intermédiaires. C'est-à-dire qu'elles ont satisfait partiellement aux exigences de la modélisation. Ainsi, la majeure partie des entreprises ne sont pas correctement préparées à la menace cyber.

La capacité du marché des cyberisques à devenir un véritable marché concurrentiel est due à un certain nombre de problèmes non résolus jusqu'à présent, ainsi qu'à des considérations pratiques. Les plus importants d'entre eux sont l'assymétrie entre les assureurs et les assurés, et la nature interdépendante est corrélée du cyberisque. L'asymétrie d'information a un effet significatif sur la plupart des environnements d'assurance et se composent de trois éléments : d'abord la capacité de l'assureur à distinguer les utilisateurs de type différent. C'est-à-dire la capacité d'effectuer une sélection adverse ou antisélection. Ensuite, un processus qui consiste à classer les assurés par groupe, afin de déterminer les primes. Et enfin, des utilisateurs ayant un comportement imprudent de nature à augmenter l'occurrence du sinistre. Cependant, nombre d'entreprises ne souhaitent pas communiquer sur leurs éventuelles vulnérabilités par crainte de voir leur réputation entachée. Ce qui aboutit une asymétrie d'information.

Dans le cadre du cyberisque, cette asymétrie est parfois trop importante. Dans ce cas, l'assureur ne dispose pas suffisamment de données lui permettant d'estimer son exposition aux risques. Ceci est parfois dû à la réticence de l'assuré à partager certaines informations qu'il juge confidentielles. Or, les assureurs doivent avoir une « fine connaissance de l'entreprise cliente pour comprendre les menaces auxquelles elles doivent faire face »[16]. À ce stade du développement du marché de la cyberassurance, l'asymétrie d'information n'encourage pas l'évolution du marché. Elle ne permet pas aux assureurs d'établir un calcul de prime adaptée aux spécificités du profit de l'assuré.

Pour être assurable, les pertes associées à un risque données doivent être estimées et modélisées grâce à l'analyse de séries historiques d'évènements passés. Cela signifie que l'estimation des risques reste fondamentale pour sa prise en charge. Dans le cas du cyberisque, les assureurs ne disposent pas d'assez d'informations sur la fréquence et la gravité des attaques cyber. La

nouveauté de ce risque fait que les calculs actuariels se basent sur des séries historiques étroites. Il s'agit, en outre, d'un risque extrêmement évolutif qui devient de plus en plus difficile à cerner.

Quand les compagnies d'assurance disposent d'un nombre de données suffisamment nombreuses, elles doivent faire face à deux contraintes techniques. D'une part, il n'y a pas de méthodologie standardisée pour inventorier de manière homogène les sinistres cyber et leur impact à l'échelle nationale et internationale. D'autre part, il existe une multitude d'organismes privés qui publient des statistiques sur les cyberattaques. À ce jour, en France, aucun organisme n'est habilité à collecter et anonymiser les sinistres cyber à l'échelle nationale afin de produire des statistiques fiables qui pourraient être partagées.

La digitalisation croissante des navires

Le transport conteneurisé ne cesse de croître en volume depuis plus de quinze ans (+ 212% entre 2000 et 2016)[17]. Une telle croissance nécessite une sécurité technologique efficace qui facilite la transparence, la rapidité et l'instantanéité. Le navire est devenu un objet traçable avec l'apport des technologies satellitaire.

Le *tracing* du navire n'est qu'un apport des technologies de l'information. La digitalisation des biens, des machines et appareils de bord, représente des centaines d'informations qui sont produites, utilisables par le bord, mais aussi par l'armateur. L'un des outils informatiques de performance et d'optimisation pour le bord, mais aussi pour les acteurs à terre, est le *monitoring*. Cet outil permet d'évaluer en temps réel des systèmes physiques par des capteurs et censeurs transmettant des informations.

Dans une étude réalisée par la *Nanyang Technological University* (NTU) de Singapour, en collaboration avec le *Cambridge Center for Risk Studies*, des chercheurs ont étudié deux scenarii de cyberattaques pour mettre en évidence leurs conséquences sur l'économie globale et le marché de l'assurance. L'un de ces scenarii, *Shen Attack*[18], concerne directement le secteur maritime. Il relève trois hypothèses de cyberattaques sur les systèmes d'information d'une société de gestion de flottes de navires ayant des connexions avec les plus grands ports de la région Asie-Pacifique. Dans la première hypothèse,

l'attaque a affecté des ports japonais, malaisiens et singapouriens. Dans la deuxième hypothèse, des ports coréens sont également touchés. Enfin, la troisième hypothèse, la plus extrême, étudie une attaque des ports chinois. Les pertes économiques subies, directement ou indirectement, sont estimées à plus de 200 milliards de dollars. Cela concerne les dommages aux marchandises périssables, mais également la suspension de la production et des exportations. Ce scénario démontre que la quasi-totalité des secteurs d'activité sont exposés, au moins indirectement, aux effets des cyberattaques. Cela s'explique par le fait que la majeure partie des entreprises utilisent les mêmes outils de stockage ou de communication, et de ce fait entraînent une corrélation des risques.

En matière d'assurance, la mutualisation des risques est un principe qui permet à l'assureur de prévoir la perte moyenne par assuré, en appliquant la loi du plus grand nombre selon laquelle l'indemnité moyen par assuré n'en est pas moins constante, lorsque les dommages sont distribués de manière identique et indépendante. Or, dans le cas des cyberisques, la dépendance des systèmes informatiques peut faire obstacle à l'application de la loi du plus grand nombre. Ainsi, un virus est capable de s'auto-répliquer dans un programme et passer d'un ordinateur à un autre en affectant les systèmes qu'il rencontre.

En outre, la vulnérabilité du système des navires ainsi que leur cyberdépendance entraîne une corrélation des risques. Cette corrélation rend la quantification du risque et la définition de la prime d'assurance beaucoup trop complexes. En effet, la proportion de contamination est trop importante ; il suffit qu'un maillon de la chaîne soit affecté pour condamner tout le système. La faille peut provenir de tout serveur ayant eu contact avec le navire ou les infrastructures à terre.

Les difficultés liées à l'assurances des cyberisques sont nombreuses. Les enjeux commandent, cependant, l'élaboration de stratégies et de solutions adaptées aux besoins des acteurs maritimo-portuaires. Une piste de réflexion pourrait provenir de la technologie des Blockchains. Sa capacité à sécuriser les données via des conteneurs numériques[19] pourrait constituer une révolution dans la maîtrise des cyberisques, tant pour les compagnies maritimes que pour les assureurs : « la piste de la blocs chaîne virgule au-delà d'une numérisation,

va introduire l'arrivée du produit d'assurance en temps réel qui pourra enfin couvrir les risques les plus incertains et complexes »[20].

Enfin, de nombreux assureurs souhaite intégrer la couverture du cyber risque dans leurs offres, soit en complément soit de façon autonome. Mais se limiter à ne proposer que des solutions assurantielles serait une erreur. Les pouvoirs publics ont un rôle majeur à jouer en la matière. Et au-delà de l'apport des Etats, les compagnies sont en mesure de s'auto-assurer. Ainsi la création d'un pool ou d'un club ne peut-elle pas résoudre le problème de capacité de l'assurance du cyberisque ?

[1] Vittel P., « Autour des rencontres parlementaires - Cybersécurité & milieu maritime », *Lettre cybersécurité et Parlement*, n°4, mars-avril 2015, p. 1.
[2] Northbridge Assurance, Qu'est-ce qu'un cyberrisque ? [en ligne] <https://www.nbins.com/fr/blog/cyberrisques/qu-est-ce-qu-un-cyberrisque/#:~:text=D%C3%A9finition%20d'un%20cyberrisque,de%20technologies%20de%20l'information.>, consulté le 20/11/2020.
[3] OCDE, *Gestion du risque numérique pour la prospérité économique et sociale : recommandations de l'OCDE et document d'accompagnement*, Éd. OCDE, Paris, 2015, p. 5.
[4] Banque de France, Evaluation des risques du système financier français, décembre 2019, p. 40.
[5] Lepetit J.-F., Rapport sur le risque systémique, Ministère de l'Economie, de l'Industrie et de l'emploi, avril 2010, p. 12.
[6] Ben Youssef W. A., Les cyber risques : nature, étendu et moyens de couverture, Lamy, Droit et Patrimoine, n° 298, 1er janvier 2020, p. 2.
[7] Ponemon Institute, 2016 Cost of Cyber Crime Study & the Risk of Business Innovation, Octobre 2016.
[8] OMI, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3, 5 juillet 2017.
[9] OMI, *Maritime Cyber Risk Management in Safety Management Systems*, MSC 98/23/Add.1, 16 juin 2017.
[10] BIMCO, *Cyber Security Workbook for Board Ship Use*, 2019.
[11] *Ibid*, p. 9.
[12] BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, *The Guidelines on Cyber Security onboard Ships*, Version 3, 2018, p. 3.
[13] Institut des Actuaires, Emergence du besoin en cyber assurance, *Compte-rendu du groupe de travail cyber*, p. 120, 2017, [en ligne] <https://www.institutdesactuaires.com/magazine/article/cyberassurance-digerer-la-part-de-risques/2549>, consulté le 19/11/2020.
[14] HM Gouvernment, Marsh, *UK Cyber Security – The Role of Insurance in Managing and Mitigating the Risk*, Mars 2015, p. 22.
[15] Hiscox, *Rapport Hiscox sur la gestion des cyber-risques 2019*.
[16] Club des Juristes, *Assurer le risque cyber*, Janvier 2018, p. 32.
[17] Banque mondiale, [en ligne] <https://data.worldbank.org/indicator/IS.SHP.GOOD.TU>, consulté le 20 novembre 2020.
[18] NTU, Cambridge Center for Risk Studies, *Shen Attack – Cyber risk in Asia Pacific Ports*, CyRiM Report, 2019.
[19] Lasmoles O., *La difficile appréhension des Blockchains par le droit*, RIDE, 2018/4, t. XXXII.
[20] Remy M., *La blockchain au service de l'assurance maritime*, [en ligne] < https://www.argusdelassurance.com/tech/la-blockchain-au-service-de-l-assurance-maritime.136654itime.136654>, consulté le 20/11/2020.

La marétique, un enjeu essentiel pour l'humanité ?

COLONEL FLORIAN MANET
Commandant de la Section de Recherches de Bretagne,
Gendarmerie nationale - essayiste

Le 28 septembre 2020, la CMA – CGM, l'un des plus puissants armateurs de porte-conteneurs mondiaux, a reconnu publiquement avoir été victime d'un rançongiciel, précédant, symboliquement, de quelques jours, l'Organisation Maritime Internationale, elle aussi victime du même mal. Auparavant, en septembre 2018, les ports de Barcelone et de San Diego en Floride ont également été perturbés par une cyberattaque. Ainsi, au travers de ces deux exemples, c'est l'ensemble de l'éco-système maritime qui est confronté à la cyber-malveillance. Reflétant aussi la numérisation croissante de l'espace maritime, cette réalité corrobore la tendance dressée par le spécialiste israélien en cybersécurité, Naval Dome1, qui avance une augmentation de 900 % des cyberattaques ciblant l'industrie navale depuis 2017. Alors s'agit- il d'une manœuvre malveillante coordonnée ciblant l'économie bleue ? Ou bien, le secteur maritime témoigne-t-il d'un déficit de prise en compte de la cybersécurité, s'exposant ainsi à de multiples attaques ?

La *marétique*, néologisme alliant la mer (mare) à l'informatique, « désigne l'ensemble des systèmes informatique et électroniques utilisés dans la gestion et l'automatisation des activités maritimes, fluviales et portuaires »2. La numérisation irrésistible de l'espace maritime sous-tend efficacement une maritimisation des échanges physiques comme immatériels ainsi que celle de nos modes de vie. Chaque cyber-crise affectant les acteurs maritimes souligne, à sa manière, le caractère stratégique du transport et des ressources maritimes à tel point qu'une marétique sécure ne peut-elle pas être considérée comme une question de survie de l'humanité ?

Dans ce contexte, l'éco-système numérique maritime aiguise les appétits d'organisations criminelles de dimension internationale en recherche permanente de profits tout comme il offre des caisses de résonance à des revendications politiques exprimées par des mouvements terroristes et, de manière dissimulée, à des États-voyous (I). La prise en otage de données et des services par ces organisations nourrit un capitalisme criminel qui prospère (II). Au total, une marétique sécure apparaît comme le garant de la résilience de la globalisation et des équilibres interétatiques (III).

Les acteurs de la marétique, entre la thalassocratie maritime3 et les terroristes

La marétique, l'ultime révolution maritime ?

Les activités maritimes connaissent depuis les années 2000 une numérisation irréfragable qui remet en cause les fondements de l'usage des espaces maritimes à l'image de l'apparition du gouvernail ou du GPS. Le navire est, désormais, pleinement intégré dans une bulle technologique mondiale qui amarre ce vecteur, jadis totalement indépendant, à un écosystème complexe, celui d'une chaîne logistique mondiale interconnectée. Dés lors, il est au cœur d'un jeu subtile d'influences assurant sa navigation, sécurisant et fiabilisant la gestion du fret, coordonnant les opérations logistiques maritimo-terrestres.

Dans ce contexte, la marétique implique l'ensemble de la communauté maritime internationale au sens le plus large. Qu'il s'agisse des communautés portuaires, des acteurs du shipping, des affréteurs, de la construction navale, de la plaisance ou de la croisière, de la pêche maritime, des énergies marines…

La numérisation croissante de l'espace maritime introduit une nouvelle dimension impalpable pour le marin. Traditionnellement, son imaginaire concevait le danger dans la violence des éléments naturels, dans l'avarie mécanique ou dans les obstacles à la navigation posés par les hauts fonds ou ceux imposés par d'autres vecteurs. Désormais, sa vigilance doit intégrer les liaisons numériques. Immatérielle par définition, cette menace invisible perturbe et se nourrit de comportements inadéquats de la part des opérateurs. Bien souvent, sa prise en compte pose problème car elle est souvent résumée à un sujet de sécurité informatique monopole de quelques experts.

D'ailleurs, le cadre légal et réglementaire propre au maritime témoigne d'une approche timide de la cybersécurité en comparaison avec d'autres sujets liés à la sécurité maritime4. A juste titre, les instances publiques régulatrices se focalisent sur la protection des données personnelles, matière sensible qui rend possible les usurpations d'identité commises à des fins illicites. Toutefois, l'internet des objets et, plus largement, l'internet industriel pâtissent d'un déficit législatif préjudiciable à la sécurité maritime.

Le cadre légal et réglementaire évoque timidement la cybersécurité

Le code ISPS5 (*International Ship and Port Facility Security*) est l'instrument réglementaire qui prévoit, de manière facultative, « *l'évaluation de la sûreté du navire devrait porter sur les (…) systèmes de radio et télécommunications, y compris les systèmes et réseaux informatiques* ». Il impose un plan de sûreté du navire comportant une cartographie logicielle et matérielle du navire, la définition des éléments sensibles et la gestion des vulnérabilités du système.

Le code ISM6 (*International Safety Management*) édicte des prescriptions génériques qui englobent les cyber-menaces sans les nommer explicitement. Il oblige les compagnies à promouvoir un environnement de travail et des pratiques d'exploitation sans danger.

L'OMI publie en 2017 des directives7 sur la gestion des cyber-risques maritimes, fournissant des recommandations pour protéger le transport maritime des cyber-menaces. Posant un premier cadre réglementaire, elle fixe aux administrations compétentes l'échéance du 1/1/21 pour la vérification de la mise en conformité des systèmes de gestion de la sécurité8 aux cyber-risques.

La norme internationale ISO 27 0019 relative aux « Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information» recense les mesures de sécurité de l'information. Elle vise à protéger les fonctions de l'entreprise et les informations de toute perte, vol, altération ainsi que de prévenir toute intrusion ou cyberattaque.

La directive européenne NIS10 prévoit la mise en œuvre de mesures destinées à assurer un niveau élevé et commun de sécurité des réseaux et systèmes d'information au sein de l'UE. Transposée en 2018 en droit français, elle identifie comme Opérateur de Services Essentiel les compagnies de transports maritimes et les gestionnaires de ports soumis à des mesures techniques et organisationnelles contre les cyber-risques.

La marétique est d'autant plus fondamentale que la communauté maritimo-portuaire affiche de multiples atours séduisant des cybergroupes criminels.
Internationale par construction, l'économie bleue rassemble de très nombreux maillons certes physiquement distants mais qu'unit une digitalisation irrésistible. Ainsi, l'affrètement d'un conteneur de 20 ou 40 équivalent vingt pieds impose l'échange d'une masse conséquente de données – un big data- entre au moins une dizaines d'opérateurs (fréteur, affréteur, compagnie maritime, autorités portuaires du départ comme de destination, douanes, sociétés de manutention, banques, …).

De plus, ces mouvements physiques de fret sous-tendent des transactions financières aux flux très divers, dissociant ce qui relèvent du transport multimodal du fret (ferroviaire, fluvial, routier), des biens transportés (vendeurs, acheteurs, metteur sur le marché, intermédiaires, apporteur d'affaire…) et enfin de la navigation maritime (compagnie maritime, services portuaires …).

Enfin, le cadre spatio-temporel dans lequel s'inscrit cette opération logistique est celui de la mondialisation. La localisation géographique des parties prenantes à ce commerce mondial reliées par le « royaume d'Archimède » suppose des fuseaux horaires différents et suggère l'absence avérée de conversation entre opérateurs en temps réel. Cet état de fait renforce l'intérêt et la pertinence de la numérisation. C'est aussi l'une des failles exploitées par les criminels.

La thalassocratie criminelle ou la maritimisation de la criminalité organisée

Les activités maritimes constituent à la fois une caisse de résonance de dimension internationale et une source de profits exceptionnels qu'exploitent méthodiquement des acteurs malveillants. Ceux-ci relèvent de trois catégories distinctes aux motivations propres : la criminalité organisée ou thalassocratie criminelle quand elle agit en mer, des mouvements terroristes et des États dits « voyous ». Si la première catégorie est uniquement mue par l'appât du gain, les deux autres agissent par idéologie et par volonté déstabilisatrice d'une organisation étatique. Quelque soit le moteur de l'attaque, les modes opératoires sont généralement identiques.

Le cyber-malfaiteur est nommé *hacker* ou pirate. L'emprunt de ce terme au monde maritime pour qualifier des faits immatériels est riche de sens tant l'analogie est possible. Même si ce phénomène ancestral n'a pas réellement changé de nature au fil des siècles, sa définition s'est, cependant, progressivement codifiée et stabilisée. L'article 101 de la Convention des Nations unies sur le droit de la mer11 définit la piraterie maritime comme « *un acte illicite de violence ou de détention ou de déprédation commise par l'équipage ou des passagers d'un navire (…) agissant à des fins privées (…) en haute mer* ». Agissant hors des eaux territoriales et hors de toute revendication politique, elle illustre le rapport inversé du faible au fort, ce que rend possible le milieu maritime. Un sommaire semi-rigide armé par un groupe de pirates peut alors défier et prendre l'ascendant sur un super tanker affrété par les majors. C'est bien là l'état d'esprit du pirate comme le suggèrent les étymologies grecque (peiratês) qui désigne « un brigand, un bandit qui court les mers pour attaquer les navires » et latine qui enrichit cet héritage de la notion de « tenter sa chance à l'aventure ». Par ailleurs, « la souplesse de l'instrument donne une prime au maître de la mer, libre d'attaquer à de multiples endroits » (Couteau- Bégarie, 1995). Remplacez « maritime » par « numérique » et imaginez un groupe cybercriminel à la place des pirates.

Les effectifs de ces pirates sont aussi incertains que le nombre d'attaques perpétrées sur les réseaux et le gain réalisé. L'analyste butte, en effet, systématiquement sur un chiffre noir12 qui dissimule une réalité en expansion. Préservant leur image, les victimes communiquent rarement sur ces attaques. Toutefois, appuyons nous sur le discours de Robert Rizika13,

représentant de Naval Dome pour l'Amérique du Nord, qui, lors d'un séminaire des opérateurs portuaires américains, évoque la réalité de la menace. Il avance le chiffre de 50 attaques en 2017 sur les réseaux d'exploitation maritime, 120 pour 2018 et 310 en 2019.

Le capitalisme criminel se nourrit de la maritimisation

Un business model fondé sur la valeur ajoutée de la data et du service
Les organisations cyber-malveillantes s'intègrent dans un système de valeurs singulier : le « capitalisme criminel ». Il dispose de règles et de ses propres codes de conduite. Dans ce marché illicite, tout s'échange et s'achète. Compétences, services, données. A l'image de l'économie réelle, des prestataires (codeurs, hébergeurs, *call-center, webdesigner*, financiers, commerciaux,…) offrent leur service sur le *darkweb* à des entrepreneurs criminels en recherche de gains à collecter sur des victimes. Un astucieux dispositif de cotation et de réputation est adossé à un système financier basé sur la confiance, la *blockchain14*. Cette confiance mutuelle acquise entre des opérateurs qui, naturellement, ne se font pas confiance est de nature à assurer la cohésion de l'ensemble.

Le paiement de la rançon par les victimes constitue le fondement de la cyberattaque. Sans lui, le système s'effondre. Il rémunère, certes, l'audacieux pirate mais, plus encore, il justifie et alimente toute une chaîne criminelle à haute valeur ajoutée qui agit en arrière fond. Crypter, coder et chiffrer des données demeurent un savoir maîtrisé par quelques *happy few* qui conservent jalousement leur talent. Dès lors, le pirate ne constituerait que la face visible d'un capitalisme criminel qui s'exprime, notamment, au travers des cyberattaques et, ce, quel que soit le mode opératoire. A l'image des enseignements tirés d'autres mécanismes criminels comme le trafic de produits stupéfiants, le malfaiteur auteur de l'infection du réseau ne serait finalement que l'équivalent de la mule qui œuvre au profit d'un commanditaire, authentique chef d'entreprise … criminelle. Reste à identifier ce cerveau capable de mettre sur le marché des solutions numériques malveillantes. Avides de gain, très opportunistes, ces organisations exploitent, avant tout, une faiblesse dans le dispositif de sécurité numérique d'une organisation. Bien souvent, elles « chalutent » les réseaux à la recherche d'une porte entrebâillée ou non verrouillée. Ainsi, l'économie bleue serait très

rarement visée en tant que telle.

Une stratégie malveillante visant l'IT et/ ou l'OT
Que les motivations soient criminelles ou politiques, la manière d'opérer consiste immanquablement à pénétrer, par ruse, effraction ou escalade, les systèmes d'informations (IT) ou d'exploitation (OT). De manière insidieuse et discrète, le pirate s'efforce, dans un premier temps, de déposer une infection sur un système, puis, dans un 2 ème temps, de mettre en œuvre ses effets (chiffrer, aspirer, contaminer, maîtriser le production d'un service) et, enfin, de signer son méfait.

IT + OT= II ?
L'IT ou technologies de l'information (*Information Technology*) désigne « tout le spectre des technologies de traitement de l'information, notamment les logiciels, le matériel, les technologies des communications et les services connexes15 ». Elles n'incluent pas les technologies embarquées qui ne génèrent aucune donnée pour l'usage de l'entreprise. Sur un navire, l'IT embarquée est constituée du réseau Wi-Fi, des VoIP, des systèmes de loisir (télévision par satellite, accès à l'Internet) et de la vidéosurveillance.

L'OT ou technologies d'exploitation (*Operational Technology*) comprend « le matériel et les logiciels qui détectent ou provoquent un changement par le biais de la télésurveillance et/ou du contrôle direct des périphériques physiques, des processus et des événements dans l'entreprise16 ». Elles concourent au bon fonctionnement de la production.
A bord d'un navire, il s'agit des systèmes de navigation électronique (ECDIS, radar), de positionnement, de géolocalisation des navires (AIS, VMS), de communication hertziens ou satellitaires dédiés au sauvetage, le système de contrôle-commande industriels (propulsion, énergie, surveillance...).
Sur un port, l'OT se traduit par le système de débarquement/ chargement des conteneurs, le *Port Community Systems*, la gestion/ positionnement des grues et portiques, la gestion des bassins (pompage, ouverture des portes..), la gestion des pipeline…

L'II ou l'Internet Industriel devient progressivement la synthèse des deux univers jadis nettement dissociés. L'analytique intelligente ou *Smart Analytics* exploite les données générées par les machines afin de modifier et d'optimiser

les processus de production. La multiplication des connectivités Internet fait muer des circuits fermés par construction vers des systèmes plus ouverts et interdépendants, générant de nouvelles problématiques de sécurité aussi bien en mer qu'à terre. Le projet smart port s'inscrit dans cette dynamique d'amélioration des performances et de la compétitivité économique.

Étude de cas caractéristiques de cette criminalité
Les technologies de l'information sont vulnérables aux rançongiciels. Une faille de sécurité identifiée par le pirate est immédiatement mise à profit. Le chiffrement des données effectué à l'insu de son propriétaire par un *cryptolocker* s'apparente à une prise d'otage du patrimoine informationnel de l'organisation cible. Cette perte de la pleine souveraineté de ces données se traduit en rebond par la perte totale ou partielle de ses capacités opérationnelles. La comptabilité, le paiement des salaires, la gestion des ressources humaines, le suivi des commandes, les fichiers clients ... peuvent être, ainsi, très perturbés voire rendus inopérants. La restauration de cette souveraineté est conditionnée par le paiement d'une rançon effectué sur la *blockchain*. A moins que des services de remédiation aient réussi à casser préalablement les codes de chiffrement.

Les réseaux on shore des armements hackés ...

Le géant du transport maritime CMA CGM Group a été la cible d'intrusion dans ses systèmes. Le 28 septembre 2020, l'accès externe à ses applications informatiques a été suspendu du fait d'une cyber-attaque impactant ses serveurs périphériques. Initiée sur la branche Asie, la compagnie maritime a suspendu l'accès externe aux applications dès la détection de la faille de sécurité.

… comme ceux d'opérateurs portuaires
Le rançongiciel Not Petya infecte le 27 juin 2017 quelques 50 000 terminaux de MAERSK. Il obligea cet opérateur mondial à une reprise manuelle de la gestion / manutention de ses terminaux à conteneurs répartis sur 600 sites de 130 pays. Au delà du délai nécessaire à la restauration de ses réseaux, les pertes directes supportées par MAERSK sont estimés à 300 millions de dollars.

En outre, les technologies d'exploitation s'intègrent dans un système de plus en plus ouverts. Les parties prenantes sont très diverses. Au delà de l'équipage, les intervenants de la maintenance agissent en physique lors d'une escale ou à distance lorsque le vecteur est en mer. Ceci induit une révolution dans la psychologie du marin pour qui la terre ferme a constitué un refuge face aux aléas naturels et aux avaries. Désormais, un logiciel malveillant ou maliciel installé lors d'une escale peut infecter des réseaux et produire ses effets une fois le navire en mer.
La malveillance attachée aux technologies d'exploitation prend différents visages : prise de contrôle à distance des fonctions essentielles à la navigation ou au système portuaire, émission d'informations fausses de positionnement géographique, manœuvre de déstabilisation des organisations ... Ses effets perturbent les opérations et la production en mer comme à terre, affectant aussi bien les flottilles que les infrastructures logistiques à terre. Ils concourent aussi à la dissimulation d'activités illicites (rejet volontaire d'hydrocarbures, non-respect d'embargo...) à l'image des brouillages du système automatique de positionnement des navires (AIS), portant atteinte à la sécurité de la navigation maritime.

Expérience de prise de contrôle à distance d'un navire par l'industriel israélien Naval Dome
Le porte-conteneurs de 260 mètres ZIM GENOVA a fait l'objet d'une expérience complexe de cyber-malveillance en décembre 201717. A la suite d'une infection de l'ordinateur du capitaine par un e-mail, une équipe d'ingénieurs est parvenue à compromettre le système de navigation du navire, les radars ainsi que les systèmes de gestion de la salle des machines.
Les effets de cette intrusion traduisent la vulnérabilité des technologies embarquées : déroutement du vecteur de sa route initiale, modifications des informations radars en passerelle en inhibant les systèmes d'alerte ou l'analyse humaine, désactivation des moteurs, des systèmes de gestion des ballasts, des jauges de soutes comme du gouvernail.

Falsification des données de positionnement afin de contourner un embargo : cas du *Yuk Tung* et du *Océan Explorer*
Le rapport du panel d'experts des Nations unies18 émet des suspicions de transbordement illicite d'hydrocarbure, hors des eaux territoriales, impliquant deux navires, le *Yuk Tung* et le *Océan Explorer*. Une opération de déception

minutieusement conçue a été constatée par un État-membre le 28 octobre 2018. Les investigations révèlent précisément le mécanisme frauduleux.

Le 22 mai 2018, en mer de Chine orientale, le *Yuk Tung* falsifie son identité maritime, se faisant passer pour le *Maika*, battant pavillon Panama. L'AIS associé émet de fausses informations relatives à sa route. Le *Maika* résulte d'une autre opération de confusion: un navire destiné à la casse, le *Hika*, pavillon des Comores, est à l'ancre à Lomé dans le Golfe de Guinée, 7000 nautiques plus loin. Pour son dernier voyage, le *Hika* se transforme en « *Mahika* » notamment sur l'AIS puis en « *Maika* »19. En réalité, le *Hika* jette définitivement l'ancre au Bangladesh pour destruction le 9 octobre 2018.

Cette usurpation d'identité maritime permet alors au *Yuk Tung* d'opérer sans attirer l'attention des services maritimes, de l'État du pavillon comme de l'État du port. La confusion du *Yuk Tung* avec le *Haika* est totale. Au delà de l'émission AIS falsifiée, ces deux navires ne font plus qu'un : l'apparence physique les rend comme des sister ships construit au même chantier naval; les marquages réglementaires apparaissent identiques sur la coque comme sur les superstructures ; le *Yuk Tung* présente un faux ou contrefait document d'immatriculation au pavillon de libre immatriculation de la République de Guinée équatoriale. Ce dispositif de déception rend donc peu suspecte une opération de transbordement entre le *Yuk Tung* et le *Océan Explorer* le 28 octobre 2018, soit 3 semaines après le désarmement du *Haika*.

Fraude aux Faux Ordres de Virement (FOVI) ou *friday afternoon fraud*: Une extorsion de fonds habillée sous les atours d'une transaction réelle s'inscrit à la suite d'un process préalable de social *engeneering*. Arguant d'une transaction à réaliser dans l'urgence, les escrocs développent une mise en scène réglée minutieusement sur le fondement de mécanismes psychologiques impitoyables. Le FOVI est un outil de déstabilisation financière qui affaiblit les opérateurs de l'industrie maritime, abusant de l'intégrité de données disponibles en source ouverte.

La marétique, garant de la résilience de la globalisation et des équilibres internationaux ?

Un risque majeur pour la navigation maritime ?

Par construction, la navigation maritime se développe au fil d'une numérisation irrésistible qui tisse un faisceau de liens immatériels interdépendants de plus en plus denses entre vecteurs mais aussi entre les vecteurs et les infrastructures portuaires.

L'enjeu premier est celui de la sécurité de la navigation maritime dans un contexte de gigantisme des unités du commerce, de la croisière … et de concentration des flottilles sur des autoroutes des mers reliant des hubs internationaux. Les falsifications de positionnement des navires du type AIS, les prises de contrôle à distance de fonctions essentielles à la navigation maritime (gouvernail, propulsion, énergie …) constituent des générateurs d'événements de mer (collision, talonnage, avarie mécanique,…) dont les conséquences peuvent être irrémédiables sur l'écosystème maritime (rejet d'hydrocarbures ou de matières dangereuses) ou perturber durablement la navigation (obstacles à la navigation type conteneurs à la dérive ou épave). En mer, les conséquences se trouvent systématiquement amplifiées et démultipliées à la fois dans l'espace comme dans le temps. L'exemple funeste produit par des marées noires en atteste.

Se pose alors la question de l'établissement des responsabilités. Certes, bien souvent, l'origine d'une cyberattaque repose sur un défaut d'intervention humaine adéquate. Même s'il convient d'admettre que le *hacker* agit par ruse ou tromperie, rendant la détection du stratagème particulièrement complexe. C'est un axe régulièrement poursuivi par les compagnies d'assurance qui, d'ailleurs, s'engagent avec une grande prudence sur la couverture du risque cyber. L'actuelle numérisation de la navigation maritime interroge sur la pleine maîtrise par l'homme de cet écosystème complexe et de ses conséquences. Le capitaine est-il encore maître de son propre navire et de son comportement à la mer tant l'Internet Industriel prospère dans les coursives et salles des machines ? Ainsi, émerge, dans le brouillard d'une digitalisation galopante et dans le spectre potentiel du navire autonome ou du navire sans équipage, le concept flou de cyber-navigabilité. En effet, le fréteur doit mettre à disposition de l'affréteur un navire en bon état de navigabilité, ce qui induit des garanties en matière de cybersécurité. Or, un

navire dont le système informatique ou l'équipage contreviendrait aux exigences en matière de cybersécurité pourrait-il être considéré comme innavigable ? La gravité de cette interrogation résonne avec les enjeux financiers d'une expédition maritime et de la valorisation du fret transporté.

Le spectre d'un chaos socio-économique ?

Le transport maritime constitue le centre de gravité des chaînes logistiques mondiales et supporte plus de 90 % du commerce extérieur. Sécuriser l'expédition maritime, c'est contribuer à garantir la régularité des approvisionnements d'économies fonctionnant à flux tendus. Or, cette mécanique internationale ne souffre pas d'à-coup ou de perturbations durables comme en ont témoigné les effets de la piraterie maritime dans l'océan Indien ou la crise sanitaire de la COVID. Cette désorganisation des chaînes logistiques se répercute systématiquement au plus profond des territoires et impacte, à des échelles différentes, les populations. A terme, fragilisant les organisations humaines, étatiques ou non-gouvernementales, ce sont les équilibres internationaux qui peuvent être remis en cause, générant des tensions. Au total, sécuriser la navigation maritime, fiabiliser l'activité portuaire et l'exploitation des espaces maritimes contribuent à renforcer la résilience d'économies tributaires du fait maritime. Alors pourquoi ne pas promouvoir une flotte labellisée « cyber-résiliente » au sein des Opérateurs de Service Essentiel afin d'assurer la continuité des approvisionnements stratégiques sous pavillon national ?

Étude d'impact20 du risque cyber sur le fonctionnement des ports et ses conséquences sur l'économie mondiale

L'étude envisage une attaque systémique des systèmes d'information en service dans une quinzaine de ports maritimes d'importance en Asie-Pacifique. Elle met, aussi, en avant les conséquences sur la *supply chain* et le commerce mondial.

Scénario	Pays des ports touchés	Nombre de ports	Total des pertes économiques en billions de dollar	Pertes économiques directes	Pertes économiques indirectes
S1	Japon, Malaisie, Singapour	6	40.8	25.7	15.1
S2	+ Corée du sud	9	55.9	36.8	19.1
X1	+ Chine	15	109.8	83.7	26.1

Fig.1 : évaluation des pertes économiques générées par une cyberattaque majeure affectant les systèmes d'information de ports situés en Asie-Pacifique selon 3 scénarii.

Les enseignements majeurs sont les suivants :
- les secteurs les plus impactés sont les transports, l'aviation, la vente au détail, la fabrication, l'immobilier, la construction,
- les pertes de productivité affectent les pays qui entretiennent des relations commerciales bilatérales avec l'un des ports infectés. L'Asie (26 billions de dollar) est la plus touchée suivie de l'Europe (623 millions de dollar) et enfin de l'Amérique du nord (266 millions de dollar),
- les pertes affectant le secteur de l'assurance sont évaluées à 9 % des pertes totales. Cela traduit la faible prise en compte du risques cyber par les assurances.

La chaîne logistique maritime mondiale est au cœur d'un complexe système reliant des économies interconnectées et interdépendantes. Une globalisation réussie repose sur une maritimisation assurée. Sans nul doute, la numérisation des systèmes d'exploitation portuaire ou *off-shore* comme ceux des navires ont contribué très largement à la meilleure rentabilité des escales, au suivi précis du fret comme des navires, à la livraison de biens au bon moment au bon endroit. Ces avancées se sont naturellement répercutées sur de multiples secteurs de l'économie. Elles ont assurément facilité la spécialisation continentale des étapes de valorisation et de transformation des ressources, de fabrication de biens de consommation. Néanmoins, cet ensemble repose

sur des fondations bien fragiles bien qu'une prise de conscience d'une meilleure cybersécurité soit effective.

La marétique apparaît comme un maillon essentielle fondant la réussite de la globalisation et la stabilité des équilibres internationaux. Confrontée à de multiples défis, l'économie bleue doit tirer les enseignements de cette nouvelle révolution fondamentale affectant l'aventure maritime : la numérisation et, son corollaire, la protection de la donnée. Puissance maritime par excellence, la France a un rôle moteur à jouer dans ce chantier au plan international. N'est-ce pas là une occasion unique de rassembler, autour de cet enjeu vital, les français, des territoires comme des littoraux ?

De la sensibilisation aux actions engagées pour la cybersécurité maritime

FRÉDÉRIC MONCANY DE SAINT-AIGNAN
Président, Cluster Maritime Français

Il y a maintenant un peu plus de trois ans, dans un édito de la newsletter du Cybercercle à l'occasion de la 3e édition des Rencontres Parlementaires Cybersécurité & Milieu Maritime, j'évoquais que « la totalité du spectre maritime (de la terre à la mer, du militaire au civil) est concerné » par les questions de cybersécurité.

A cette époque, beaucoup parmi les acteurs du monde maritime se croyaient à l'abri. Malgré cela, dès 2016 le Cluster Maritime Français représenté par Alexandre LUCZKIEWICZ, organisait nos premiers ateliers de sensibilisation à la cybersécurité maritime (risques économiques, espionnage industriel, PCA/PRA, l'assurance du risque cyber, les connexions mer/terre, etc.). De même l'ANSSI et la Direction des Affaires Maritimes publiaient des guides d'hygiène informatique et de renforcement de la sécurité numérique des navires, et (encore timidement) l'Organisation Maritime Internationale (OMI)[1] commençait à considérer les recommandations de l'ENISA (European Union Agency for Cybersecurity) et du BIMCO (Baltic and International Maritime Council)[2].

Aujourd'hui, 3 ans plus tard, où en sommes-nous ?

Sans être alarmiste, mais simplement réaliste, de récents évènements nous l'ont montré, nous devons considérer que les acteurs des différents secteurs de la filière maritime ont été, sont ou vont être victimes de cyberattaques. Celles-ci sont de plus en plus sophistiquées, massives ou ciblées, envers une filière industrielle hautement stratégique tant sur le volet naval que civil, on l'a encore vu durant les 2 épisodes de confinement dû à la crise Covid19 et particulièrement en matière de capacité d'approvisionnement du Pays par le

transport maritime et via nos ports. Plus que jamais, le maritime est identifié comme un secteur stratégique et la vigilance est de mise.
Les exemples très récents nous prouvent que ce n'est pas que l'ordinateur personnel de Monsieur-tout-le-monde qui est visé, mais bien de grandes organisations telles l'OMI, ou encore un grand armateur mondial, ou encore un port de commerce, qui sont des cibles privilégiées, avec une volonté manifeste de nuire, au-delà du classique *ransomware*. Il s'agit clairement d'actes de guerre économique.

Les infrastructures complexes telles les infrastructures portuaires ou les navires sont donc par essence des unités à préserver.

De la nécessité d'une gouvernance cyber maritime…

Passé la sensibilisation (qui mérite pourtant encore d'être acquise comme une priorité de rang 1 au sein des entreprises), comment pouvait-on réagir ?

C'est dans cette objectif, s'appuyant sur la mesure 37[3] du Comité Interministériel de la Mer de 2017 (CIMER) et la mesure 46[4] du CIMER de 2018 relatives à la gestion du risque cyber, qu'au sein du Comité France Maritime[5] a été créé un atelier dédié, et qu'un coordinateur cyber a été nommé pour mener à bien deux missions : d'une part rédiger une cartographie des besoins et des solutions existantes en matière de cybersécurité, au profit des acteurs du maritime, et d'autre part de travailler à établir une stratégie nationale cybermaritime.
En complément, une veille sur des actualités et événements sensibles mais « visibles » était effectuée, et récapitulée au travers de lettres mensuelles d'information cyber du monde maritime.
Au terme de cette mission, deux actions prioritaires ont été engagées :
Tout d'abord, la création en novembre 2019 d'un modèle de gouvernance cyber du secteur maritime, appelé C2M2, pour « Conseil Cyber pour le Monde Maritime ».
Cette instance a pour vocation de réunir les acteurs français du monde maritime dans une même enceinte pour échanger sur la réglementation actuelle et future relative à la cybersécurité et pour porter, par l'intermédiaire du conseil, la voix de la France dans ce domaine au niveau européen et mondial. Il dispose d'un Comité Exécutif (COMEX) avec deux collèges

(institutions et opérateurs), qui valide une stratégie cybersécurité pour le domaine maritime et donne les axes de travail. En outre, deux sous-comités « analyse des risques » et « prospective et régulation », ont été mis en place ainsi qu'un groupe de travail dédié au « port sécurisé » :

- Le sous-comité « prospective et régulation » est chargé d'identifier les actions pertinentes à conduire dans les domaines techniques, normatifs et réglementaires et interagir avec les instances internationales et les institutions européennes pour y défendre nos intérêts nationaux.
- Quant à lui, le sous-comité « analyse de risques » s'astreint à identifier les risques du secteur maritime et à tenir à jour le tableau de bord des risques cyber.
- Enfin, le groupe de travail « port sécurisé » suit au plus près le projet national de sécurisation et de coordination des plateformes portuaires, projet qui a d'ailleurs été proposé comme projet structurants des « territoires de confiance » au sein du comité stratégique de filière des industries de la sécurité.

Les objectifs principaux du « Conseil Cyber pour le Monde Maritime » sont d'identifier les projets structurants pour la filière maritime dans le domaine de la cybersécurité et d'établir avec les acteurs des différents secteurs du maritime une stratégie ainsi qu'une feuille de route pour les prochaines années.

… aux actions concrètes

Ensuite, et c'est relié aux décisions du C2M2 , la deuxième action est la création d'un Centre de Coordination Cyber du Monde Maritime, appelé « France Cyber Maritime », dont la présentation officielle a été récemment faite lors du CyberHub by FIC à l'occasion du salon Euronaval Online 2020.

France Cyber Maritime sera créée sous la forme d'une association Loi 1901 et devrait voir le jour d'ici la fin de l'année 2020. Elle comportera plusieurs collèges répartis autour des « organismes publics et territoriaux » « des apporteurs de solutions » et des utilisateurs. L'association travaillera sur de nombreux projets, au travers de trois types d'activités :

- D'abord, une activité associative, qui répond principalement à une mission de service public de recueil, d'expertise, d'appui, et de gestion des incidents

pour l'ensemble des acteurs du domaine (conseil technique des administrations, mise en œuvre des services de prévention, de partage d'informations et de gestion des incidents).
- Ensuite, une activité de mise en place de contrats co-financés, de missions de service public de capitalisation et de perfectionnement des connaissances, de formation et de recherche (prestations contractées avec les membres de l'association et contrats à financement partiel avec les entités publiques) ;
- Et enfin une activité de prestations extérieures au travers de contrats de droit commercial ou de marchés publics passés entre l'association et des entités externes (publiques ou privées).

Parmi les projets-phares de France Cyber Maritime, on pourra noter la mise en place d'une analyse de la menace au travers d'un *Maritime-SOC*[6], et qui s'appuiera sur un *Maritime-CERT*[7] qui quant à lui assurera les missions de veille, de diffusion, d'alerte et partage d'informations, mais aussi la centralisation et la gestion des incidents, ainsi que la coordination de la réponse aux incidents identifiés.

Autres projets, la structuration d'une offre de formation initiale (relatif à la sensibilisation, à la formation et à l'entrainement) et de formation continue (par le biais d'un Mastère spécialisé[8]), ainsi qu'une offre de conseil (audit, accompagnement) aux entreprises et institutions.
Sur le volet R&D et innovation, des offres de services seront proposées pour répondre au plus près des besoins des industriels sur le plan tant national qu'international.

Dans le cadre des contrats stratégiques de la filière des industriels de la sécurité ou de celle des industriels de la mer, ou encore dans le cadre du plan de relance l'incubation des futurs projets devrait être portée par l'association France Cyber Maritime en lien avec le futur Campus Cyber voulu par le gouvernement. Les projets qui seront développés au sein de ce centre de coordination « cybersécurité maritime », qui devra monter rapidement en puissance grâce aux financements publics et privés ainsi qu'à l'implication de services de l'Etat, contribueront à faire de cet organisme le lieu de référence en matière d'innovation grâce à la diversité des compétences et des données qui y seront rassemblées.
Gageons désormais qu'après ces années de sensibilisation des acteurs du

monde maritime, puis les actions concrètes décrites ci-dessus, notamment au travers de la mise en place d'une gouvernance impliquant les services de l'Etat et les différents secteurs du privé, que la filière maritime puisse maintenant mieux appréhender la cybersécurité, de manière globale et systémique.

Il faut continuer collectivement ce travail pour connaître et comprendre les risques cyber auxquels nous devons faire face, à terre et en mer, pouvoir les anticiper, pouvoir y répondre, notamment à l'aide d'un outil fonctionnel et coordonné, à l'image des centres de cybersécurité maritime successivement et récemment créés aux USA, au Royaume-Uni, en Estonie et prochainement en Norvège, c'est ce à quoi va s'employer France Cyber Maritime sous l'égide du Conseil Cyber pour le Monde Maritime.

[1] Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3), issued on July 2017 and IMO Resolution MSC.428(98) : Maritime Cyber Risk Management in Safety Management Systems, adopted in 16 June 2017

[2] https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[3] L'État complète et adapte les mesures de sûreté maritime et portuaire dans tous les champs nécessaires : consolidation des moyens de réaction de l'État face à un incident « cyber » à bord d'un navire marchand battant pavillon français.

[4] La France prend toute la mesure des enjeux liés à la cybersécurité dans le domaine maritime, à la fois en termes de protection des systèmes d'information et en termes de développement économique d'un secteur et décide ainsi la création d'une Commission cybersécurité et la préfiguration d'un centre national de coordination de la cybersécurité pour le maritime.

[5] Le Comité France Maritime (CFM) est une instance informelle public-privé qui rassembles les services de l'Etat, les Régions et les fédérations professionnelles des différents secteurs du maritime, pour :
- Lever les obstacles qui freinent le développement économique
- Identifier et prioriser les actions à porter dans le cadre des politiques publiques de l'Etat, en vue du Comité Interministériel de la Mer
- Accompagner et mobiliser les différentes catégories d'acteurs (privés et publics)

Le CFM est co-présidé par le Secrétariat Général de la Mer et le Cluster Maritime Français

[6] Security Operations Center

[7] Computer Emergency Response Team

[8] Création début 2020 du Mastère spécialisé "Cybersécurité des systèmes maritimes et portuaires" porté par quatre Grandes Ecoles (IMT Atlantique, École Navale, ENSTA Bretagne et l'ENSM)

Autopsie des cyberattaques et des moyens de s'en protéger par le dispositif national de prévention et d'assistance Cybermalveillance.gouv.fr

JÉRÔME NOTIN
Directeur général, Cybermalveillance.gouv.fr

Après Maersk en 2017, puis plus récemment Carnival et CMA CGM en 2020, qui ont été des exemples concrets et médiatisés, les acteurs du secteur maritime, quelle que soit leur taille, n'ont pas été épargnés par les cyberattaques ces dernières années.

Mais qu'est-ce réellement qu'une cyberattaque ? Quelles sont les motivations des cybercriminels ? Quelles peuvent être les conséquences pour les victimes ? Comment se protéger ? Cybermalveillance.gouv.fr vous donne des éléments de réponse ainsi que son apport possible aux acteurs du secteur.

Le numérique, terrain d'opportunités bienveillantes... et malveillantes

Aujourd'hui, le numérique a pris une place fondamentale dans notre société. En permettant de partager et d'échanger de l'information depuis n'importe quelle partie du globe en quelques secondes, le numérique a ouvert le champ des possibles entre les individus et les organisations. Les opportunités créées par la dématérialisation de l'accès à l'information et des procédures peuvent être considérées comme un progrès qui facilite les interactions entre les personnes, les administrations, les entreprises. Cette dématérialisation est toutefois vue également comme une opportunité pour des acteurs criminels. En effet, grâce au numérique dont ils maîtrisent les biais, ils peuvent également intervenir à distance, de manière furtive et rapide, pour commettre divers méfaits qui servent leurs intérêts, avec une créativité sans cesse renouvelée.

Entre opportunités et dangers, l'espace numérique peut donc s'apparenter au «*grand Ouest*» de la ruée vers l'or, pour le meilleur comme pour le pire.

Cyberattaque versus cybermalveillance

L'acception généralement admise d'une cyberattaque est une attaque commise par des moyens numériques et visant à atteindre de manière illicite d'autres moyens numériques, pour accéder à leurs informations et/ou en perturber le fonctionnement normal. Si les cyberattaques font partie intégrante des cybermalveillances, les cybermalveillances ont un champ d'application plus large. Elles recouvrent non seulement les cyberattaques qui visent les systèmes numériques, mais également les attaques qui visent leurs utilisateurs, que ce soit pour les escroquer ou fausser leur jugement. Force est toutefois de constater que les deux appellations ont tendance à s'assimiler, voire se confondre dans le langage commun, et que c'est un fait qu'il vaut mieux accepter plutôt que contester, au risque que la préoccupation sémantique n'obère la réalité du sujet. En effet, qu'il s'agisse de cyberattaque ou de cybermalveillance, ces deux notions recouvrent toujours des faits délictueux et infractionnels commis par voie numérique qui peuvent donc être poursuivis et réprimés comme tels.

Principales cyberattaques

À ce jour, le dispositif Cybermalveillance.gouv.fr répertorie plus de 40 types de cybermalveillances pour lesquels il propose conseils, assistance et orientation des victimes. Parmi ces menaces, l'hameçonnage (*phishing* en anglais) arrive en tête des risques pour les entreprises. En usurpant l'identité d'un tiers ou service de confiance, cette attaque cherchera à obtenir des informations sensibles (exemple : mots de passe) permettant d'accéder frauduleusement aux systèmes numériques de l'entreprise et est souvent la phase qui précède des attaques d'impacts plus importants. Viennent ensuite les attaques par rançongiciels (*ransomware* en anglais), dont la presse se fait régulièrement l'écho et qui peuvent avoir de très fortes conséquences pour les victimes. Ces attaques chiffrent les données des entreprises et leur demandent une rançon pour en récupérer l'accès. Elles sont généralement précédées d'une intrusion à distance dans le réseau de l'entreprise et d'une destruction de ses sauvegardes, mais également de plus en plus fréquemment d'un vol de données et d'une

menace de les rendre publiques pour accentuer la pression et augmenter le montant des rançons. Enfin, arrivent au cœur des préoccupations les différents types d'escroqueries, souvent très bien réalisées et documentées, qui cherchent à profiter de la dématérialisation des procédures, comme les «arnaques au Président» qui demandent un virement urgent et confidentiel en usurpant l'identité d'un dirigeant, ou encore les arnaques au changement de coordonnées bancaires d'un fournisseur.

Les cybercriminels ou l'appât du gain

Bien qu'en déclin, l'activisme idéologique ou politique popularisé par des groupes comme les «*anonymous*» ou les divers «*cyberdjihadistes*» ne s'est pas complètement éteint et représente toujours un risque pour les organisations. Toutefois, ce segment a progressivement laissé la place ces dernières années à des activités cybercriminelles aux motivations principalement financières. Aujourd'hui, l'image d'Épinal du jeune prodige en informatique qui piratait le réseau d'une entreprise avec pour seul objectif d'obtenir la reconnaissance de ses pairs est quasi révolue. L'Internet parallèle que représente le *darkweb* a permis de voir des individualités, motivées par l'appât du gain, se regrouper pour agir de concert, jusqu'à former de véritables cartels cybercriminels organisés en domaines de spécialités, de la conception d'outils d'attaque, à leur utilisation, en passant par leur commercialisation et au blanchiment des fonds récupérés. La cybercriminalité s'est donc professionnalisée et les entreprises doivent à présent faire face à des niveaux de sophistication d'attaques qui s'apparentent à celles que pouvaient autrefois seuls conduire des services de renseignement étatiques dans la sphère géopolitique. Cette hydre cybercriminelle pouvant aller jusqu'à louer ses services au plus offrant pour des opérations de déstabilisation ou d'espionnage économique.

Nul n'est à l'abri

Considérer que l'on pourra être épargné par les cyberattaques est une erreur à ne plus commettre. L'actualité démontre régulièrement que tout un chacun peut se retrouver ciblé, que ce soit à titre individuel ou collectif, au sein des entreprises ou des organisations. Hôpitaux, laboratoires, communes, collectivités, associations, ONG, entreprises de toutes tailles sont ainsi frappés quotidiennement, que ce soit de manière aveugle ou particulièrement ciblée.

La question n'est donc plus pour les organisations de savoir si elles seront frappées, mais quand. Et si tant est qu'elles ne le soient pas déjà sans le savoir, comment s'en prémunir au mieux. La politique de l'autruche ne semble donc plus permise sous peine de mettre en danger la sécurité de son organisation, mais aussi de celle de ses utilisateurs, clients, partenaires.

Conséquences des cyberattaques

Les conséquences d'une cyberattaque peuvent s'avérer dramatiques et pas seulement pour l'entreprise qui la subit. Si, dans le cadre d'une escroquerie, il peut s'agir avant tout d'une perte financière directe dont une entreprise fragilisée peut avoir des difficultés à se rétablir, dans le cas d'une atteinte à ses systèmes numériques les conséquences sont multiples. En premier lieu, cela occasionne généralement un arrêt du système attaqué et sa remise en service sécurisée peut parfois prendre des jours, voire des semaines. Cette situation occasionne non seulement des pertes d'exploitation, mais également un engagement de ressources humaines et financières important et imprévu pour la rétablir. De même, une cyberattaque est généralement découverte (tôt ou tard) par l'opinion et l'impact négatif sur les clients, les investisseurs et les partenaires de l'entreprise victime est toujours réel, car il altère la nécessaire confiance et crédibilité. Enfin, l'entreprise victime doit considérer qu'elle n'est certainement pas la seule à avoir été impactée directement ou indirectement par la cyberattaque qui la frappe. Les interconnexions qu'elle peut avoir avec ses partenaires peuvent également leur propager l'attaque et les mettre en danger. Tout comme elle peut mettre en danger la sécurité des informations de ses clients, voire de ses collaborateurs qui ont pu être détournées. Sans compter les risques qui pourraient peser sur des vies humaines si des systèmes numériques rendus indisponibles ou défaillants pouvaient les impacter. Dans ce cadre, l'entreprise victime peut également avoir à devoir affronter des recours juridiques si sa responsabilité ou sa défaillance peuvent être mises en cause. Dans une cyberattaque, une entreprise peut donc jouer jusqu'à sa survie et entraîner avec elle ses parties prenantes directes ou indirectes dans un effet domino.

Causes des cyberattaques

La cause d'une cyberattaque est toujours l'exploitation d'une faille par les

attaquants dans la sécurité de la victime. Contrairement à ce que qu'on pourrait ou voudrait penser, les failles exploitées sont plus souvent humaines que directement techniques. En effet, les failles généralement qualifiées de «techniques» relèvent en fait d'un défaut d'utilisation de la technique et non de la technique elle-même. Les attaquants vont ainsi principalement chercher leurs portes d'entrée dans l'exploitation d'une vulnérabilité logicielle non corrigée (alors qu'elle aurait pu l'être), un défaut de configuration d'un équipement de sécurité, un manque d'hygiène dans la gestion des mots de passe, un défaut de moyens et de procédures de contrôle, voire une trop grande précipitation et un manque d'attention des utilisateurs, pour ne pas dire dans certain cas une certaine forme de négligence coupable. On peut ainsi s'être offert la plus belle porte blindée du monde, si on ne sait pas l'utiliser, on l'utilise mal, voire on laisse la porte ouverte, elle ne sera d'aucune utilité pour se protéger. C'est souvent partant de ce postulat que les attaquants pourront commettre leurs actions.

Cybersécurité : revenir aux fondamentaux

La cybersécurité est avant tout une affaire de bon sens, d'humilité et d'acceptation de contraintes. De bon sens, car une grande majorité des cyberattaques pourrait être évitée si des mesures sommes toutes assez simples étaient mises en œuvre : comme une bonne gestion des mises à jour de sécurité, des sauvegardes et des mots de passe. D'humilité, car personne n'a jamais su construire une forteresse imprenable et il en va de même avec ses systèmes numériques. Quelles que soient les solutions techniques et le budget déployé, il faut continuer à agir en ayant conscience que le risque subsistera toujours, il sera juste minimisé. Il faudra donc non seulement déployer des systèmes de sécurité (antivirus, pare-feu…), mais également mettre en place une supervision pour détecter les attaques qui pourraient réussir à les traverser afin de pouvoir les enrayer avant qu'elles n'occasionnent des dégâts irréversibles. Bien entendu, la cybersécurité a un coût humain et financier qu'il faut accepter proportionnellement aux risques et aux dommages qu'une attaque pourrait causer sur l'organisation qui en sera victime.

La sensibilisation, une arme de protection massive

La sécurité est généralement vécue comme une contrainte et n'est donc

efficace que si elle est comprise et acceptée. La défaillance humaine étant la principale cause des cyberattaques réussies, c'est par la sensibilisation et la formation des acteurs que l'on pourra minimiser les risques. L'humain doit donc être mis au cœur du dispositif de détection, de réaction et de préservation de la sécurité de l'organisation. Mais l'humain est souvent résumé à l'utilisateur lambda, ce qui est une grave erreur. Certes, cet utilisateur a toute sa place dans cette démarche, mais pas moins que les techniciens et les informaticiens, fréquemment oubliés mais sur lesquels repose pourtant une grande partie de la sécurité. Sans compter les cadres et dirigeants qui sont d'autant plus des cibles de choix qu'ils peuvent avoir tendance à éluder les mesures de sécurité qu'ils ont eux-mêmes édictées. Pour aider les organisations à assurer la formation et la sensibilisation de leurs personnels, Cybermalveillance.gouv.fr propose gratuitement de nombreux supports pédagogiques telles que des fiches sur les principales menaces et mesures pour y faire face, les bonnes pratiques élémentaires ainsi que des infographies, des vidéos, des kits…

Savoir se faire accompagner

Un système qui fonctionne n'est pas a priori un système sécurisé pour faire face aux attaques. Sécuriser un système ou une infrastructure numérique requiert des compétences spécifiques dont les organisations ne disposent que rarement en interne. Qu'il s'agisse de faire un état des lieux de sa sécurité numérique, de sécuriser ses systèmes ou de détecter les attaques, ou encore d'intervenir pour y faire face quand elles se produisent, les organisations doivent savoir se faire accompagner par des prestataires spécialisés en cybersécurité. Sur sa plateforme, Cybermalveillance.gouv.fr propose déjà aux particuliers et professionnels de les mettre en relation avec des prestataires référencés susceptibles de les assister en cas d'attaque. Pour aller encore plus loin, Cybermalveillance.gouv.fr a créé, avec le soutien de l'AFNOR et en partenariat avec des organisations professionnelles, un label destiné à donner un premier niveau de reconnaissance des compétences des prestataires de cybersécurité dans la sécurisation des systèmes numériques, leur maintien en condition opérationnelle de sécurité et la réaction sur incident. La liste des prestataires qui auront obtenu ce label, baptisé ExpertCyber, sera accessible en 2021 sur la plateforme Cybermalveillance.gouv.fr.

Cybermalveillance.gouv.fr : un partenariat public-privé au profit de tous

Cybermalveillance.gouv.fr est le dispositif national d'assistance et de prévention en sécurité numérique. Ce dispositif, voulu par l'État pour répondre aux besoins des populations, a été créé en 2017 par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) et le ministère de l'Intérieur. Il est piloté par un groupement d'intérêt public, le GIP Action contre la cybermalveillance (ACYMA), qui rassemble plus d'une quarantaine de membres - acteurs étatiques, représentations professionnelles, associations de consommateurs et d'aide aux victimes, opérateurs, éditeurs, assureurs, banques... - engagés ensemble dans la lutte contre la cybermalveillance. Cybermalveillance.gouv.fr s'adresse à toutes les catégories de publics, qu'il s'agisse des particuliers, des entreprises, des associations, des administrations ou des collectivités. Sur ces publics, les missions du dispositif sont la sensibilisation aux risques de sécurité numériques et aux bonnes pratiques, l'assistance en ligne aux victimes en cas de cybermalveillance qui va, si besoin, jusqu'à la mise en relation avec un réseau de plus de 950 professionnels référencés, et l'observation de la menace qui permet de compléter son offre de services et d'éclairer l'action publique. En 2019, plus de 90 000 personnes sont venues chercher de l'assistance sur la plateforme Cybermalveillance.gouv.fr.

Gestion de la complexité : une approche cyber

Responsable du Pôle Sécurité des Systèmes d'Information,
Direction Générale de l'Armement*

La France, en tant que deuxième espace maritime mondial, dispose d'une Marine nationale armée pour répondre à un ensemble de missions afin de préserver la paix et défendre les intérêts nationaux. Ses missions variées, de renseignement, de prévention, d'intervention, de protection et de dissuasion, doivent pouvoir être menées dans différents contextes d'intervention, dans des milieux amis ou ennemis, avec ou sans tensions internationales. Il est essentiel que ces missions puissent être réalisées dans ces différents contextes de menaces et donc potentiellement en présence de cyberattaques. La cybersécurité d'un système maritime apparaît donc comme une performance opérationnelle à part entière, et non seulement comme une contrainte réglementaire, comme cela a pu être perçu par le passé.

Pour atteindre cette performance, il est nécessaire de caractériser correctement la menace cyber. Les armes cyber apportent en effet un très large panel d'actions et permettent de se substituer, préparer, amplifier ou compléter d'autres modes d'actions pour atteindre des effets : de renseignement (évaluation des capacités adverses par le recueil ou l'extraction d'information), d'entrave (réduction ou neutralisation des capacités adverses), de déception (modification de la perception ou de la capacité d'analyse adverse). De plus, les armes cyber disposent de caractéristiques atypiques par rapport à d'autres capacités. Elles sont utilisables à distance, avec des actions non nécessairement menées au contact physique de l'adversaire. Ces actions peuvent être menées en toute discrétion et avec l'objectif de préserver l'origine de l'attaque, voir essayer de la faire attribuer à quelqu'un d'autre. Enfin, elles apportent un contrôle de la finesse et de la temporalité des effets. Les effets peuvent être

immédiats ou au contraire désynchronisés de l'attaque (conditions de déclenchement) et nécessitent un travail de préparation et de pénétration des systèmes qui peuvent avoir lieu plusieurs mois avant une réelle activation. Les armes cyber offrent également des possibilités de réversibilités, c'est-à-dire qu'elles n'ont pas obligatoirement une fonction létale sur un système : les ransomwares ne cherchent pas à détruire des données, mais à les conserver, jusqu'à paiement de la rançon.

Les systèmes maritimes et les systèmes de défense associés peuvent se définir comme des systèmes de systèmes : bâtiments principaux de combat, de défense, bâtiments support, …. Ceux-ci, tout comme la plupart des systèmes numériques civiles, sont désormais en constantes interconnexions numériques et sont de plus en plus dépendants de ces échanges. Tel une poupée russe, chaque bâtiment de surface ou un sous-marin s'apparentent à des systèmes complexes emboités les uns dans les autres et interdépendants car interconnectés : cohabitent ensemble, les différents systèmes industriels (énergies, propulsion, …), les systèmes d'information (commandement, système de télécommunication radio/satellite, …) et les différents systèmes d'armes (missiles, torpilles, systèmes de défense, …) pouvant disposer eux-mêmes de leurs systèmes de préparation de mission. Ces systèmes et équipements, anciennement cloisonnés et aux technologies non numériques, embarquent désormais une part croissance de composantes logiciels à tous les niveaux. A cela, il est nécessaire de prendre en compte les systèmes industriels de développement et de maintenance, qui, bien que non opérationnels au sens militaire du terme, sont autant de systèmes qui s'interconnectent avec les systèmes opérationnels tout le long de leur vie. Les cybermenaces tirent bénéfice de ces multiples interconnexions de systèmes, de la diversité des fonctions et des technologies embarquées, et de la malléabilité des logiciels, offrant une surface d'attaque de plus en plus grande et rendant ces systèmes, au final, plus complexes à défendre.

Face à cette complexité, il est nécessaire de s'organiser pour maîtriser les risques associés à ces activités opérationnelles. Une démarche bottom/up, partant de la sécurisation de tous les points d'accès, équipements, systèmes, demanderait des ressources financières et humaines non disponibles, et n'apporterait pas, au prix d'une énergie démesurée, une réponse à l'objectif

initial d'assurer la mission sous pression cyber. Sans être inutile, elle ne permet toutefois pas de se convaincre de la sécurité globale apportée au système vis-à-vis de sa mission. Une démarche top/down, à partir d'une compréhension des enjeux opérationnels de chaque système et sous-système, portant sur la compréhension métier de la capacité marine et de son étendue, semble plus porteuse de succès. Pour la mener à bien, il est donc nécessaire de réaliser (puis maintenir) une cartographie structurée et hiérarchisée des systèmes de la capacité, d'en identifier et mesurer les risques et d'identifier les mesures de réduction de ces risques. En menant cette démarche du point de vue de l'attaquant, en identifiant les effets recherchés sur les missions (arrêt, perturbation, entrave, …) et les modalités d'action les plus efficaces pour les atteindre (recherche du/des maillons faibles dans les systèmes de systèmes soutenant les activités opérationnelles, sur l'ensemble du périmètre, dont les systèmes support et les systèmes de soutien), les systèmes névralgiques et les risques encourus apparaissent plus aisément. Selon cet angle d'approche, Il devient alors nécessaire d'identifier :

- les événements redoutés (ou les effets recherchés par l'attaquant), priorisés par criticité, selon des besoins d'intégrité de fonctionnement, de disponibilité et/ou en confidentialité ;
- les sources de menaces cyber contre lesquelles un niveau de résistance doit être apporté ;
- le niveau d'exposition à la menace cyber (fonction notamment de la complexité, de la connectivité et des familles de technologies mises en oeuvre).

Cette démarche permet d'aboutir à l'expression du besoin de cybersécurité de niveau capacitaire, qui peut ensuite se décliner par des allocations de performances sur les différents systèmes et sous-systèmes, principaux et contributeurs. Elle permet aussi de mieux cerner les systèmes qui doivent être surveillés, soit du fait de leur criticité, soit du fait de leur trop grande exposition. L'adoption du point de vue de l'attaquant permet aussi d'identifier les enjeux de cybersécurité devant être portés sur l'ensemble du cycle de vie et sur un périmètre étendu – notamment au niveau des systèmes de développement, de qualification ou plus globalement de la chaîne d'approvisionnement (supply chain), mais aussi des systèmes de maintenance. Cette démarche permet de mettre en lumière le rôle essentiel

et parfois oublié des fonctions de support : que deviendrait un bâtiment de surface s'il ne pouvait recevoir son ravitaillement en nourriture ou en carburant lors d'une mission longue ?
Cette démarche capacitaire cyber s'applique à l'ensemble des capacités opérationnelles des Armées. Elle permet d'orienter les efforts financiers et en ressources humaines pour la sécurisation au bon niveau des systèmes participant aux missions de souveraineté. La connaissance des possibilités cyber des attaquants est toutefois un préalable à cette démarche. Celle-ci nécessite des compétences de renseignement qui dépassent le seul cadre cyber. De plus, les connaissances métiers et opérationnelles sont indispensables lors des phases d'évaluations des enjeux sur les systèmes d'armes et les risques associés. Une telle démarche ne peut donc être réalisée sans une équipe dédiée, composée d'opérationnels, garants de la compréhension métier, et d'architectes cyber, apportant la connaissance des possibilités offertes par le domaine cyber ainsi que l'approche « attaquant ».

La possibilité d'allouer des performances cyber aux différents systèmes et sous-systèmes permet une décomposition des actions et des charges de travail associés. Chaque équipe de projet peut se voir alors alloués des objectifs concrets contribuant à la sécurité de l'ensemble. Il reste néanmoins nécessaire de disposer d'une structure de pilotage et de contrôle, permettant de vérifier l'atteinte des objectifs de performance cyber requis par les différentes parties et sous-parties. Elle permet de faire intervenir les bons représentants métiers, sans devoir créer une structure trop grande.

Cette approche est complémentaire d'autres démarches de sécurisation ; elle repose sur l'existence d'une BITD (base industrielle et technologique de défense) apte à proposer des équipements et des systèmes de niveaux de sécurité permettant de faire face aux cybermenaces. Elle reste néanmoins non adhérente aux solutions (équipements, logiciels de cybersécurité) à mettre en place.

Le défi de sa mise en oeuvre repose sur les ressources à mobiliser pour initier le mouvement ainsi que sur les bons outils à mettre en place pour soutenir ce mouvement. Ces outils doivent permettre le suivi dans le

* Pour des raisons de confidentialité liées à l'identité de certains personnels de la Défense, le nom de l'auteur ne peut être indiqué.

temps de l'ensemble des informations générées par les différentes parties et le partage de l'analyse commune. Ils doivent apporter cette vision d'ensemble qui est indispensable aux forces pour maîtriser les performances cyber de leurs systèmes pour leurs opérations.

Table des matières

Cet ouvrage est le premier opus de la Collection CyberCercle que nous avons décidé de lancer cette année.

Des livres collectifs, dont chaque édition associe des auteurs représentant différentes organisations, publiques et privées, autour d'une thématique déterminée dans le champ de la confiance et de la sécurité numériques.

Des livres collectifs qui peuvent se lire de la première à la dernière page ou de façon séquencée, par des entrées « auteur » ou « thématique ».

Ces ouvrages n'ont pas l'ambition d'être exhaustifs. En revanche, grâce à des contributions de personnalités expertes complémentaires, ils ont pour vocation d'apporter aux lecteurs des éléments d'analyse de confiance, propres à enrichir leur appréhension du sujet et leur réflexion.

La Collection CyberCercle veut ainsi s'inscrire, à travers ses deux publications annuelles, comme une référence dans le panorama français de réflexion sur les sujets de confiance et de sécurité numériques, un outil de travail au service de la décision.

Ce premier opus est dédié la cybersécurité maritime, un des secteurs d'expertise du CyberCercle, secteur dont l'actualité intense nécessite aujourd'hui des éclairages pour accompagner les actions à venir.

Cet ouvrage a été réalisé avec le soutien de

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

FORTINET

GICAN

CERTitude NUMERIQUE