LETTRE
CYBER SÉCURITÉ et Politiques Publiques

CYBER CERCLE

N°1 - OCTOBRE 2018

Édito

LA CYBERSÉCURITÉ DANS LE MILIEU MARITIME : UN IMPÉRATIF STRATÉGIQUE

Le secteur maritime n'est pas épargné par les impératifs de compétitivité et de rentabilité au sein d'une économie mondialisée. Pour conserver une pertinence face à leur concurrents internationaux, les acteurs du milieu maritime peuvent trouver des gains d'efficience dans une stratégie de numérisation des flottes. Dans cette logique, nombreux sont ceux à s'être emparés des innovations numériques en modernisant leur système de gestion des cargaisons, les outils de navigation, les systèmes de contrôle ou alors les outils de surveillance. Les systèmes informatiques permettent en effet aux navires de naviguer avec des équipages réduits, et d'assurer ainsi les mêmes missions à moindre coût.

Toutefois, cette modernisation expose également le secteur maritime à de nouveaux cyber-risques. La mise en réseau croissante des systèmes d'information les rend vulnérables face à d'éventuelles intrusions, via les communications internet ou des clés USB notamment. Le domaine de la défense a déjà saisi ces enjeux depuis plusieurs années, mais le secteur civil peine encore à les intégrer dans ses démarches de sécurité. Par ailleurs, une véritable prise de conscience s'opère dans l'enseignement avec, par exemple, la création de la chaire de cyberdéfense des systèmes navals à l'École navale de Brest.

Pour faire face à ces nouvelles menaces, il est impératif, d'une part, de procéder à une évaluation et une certification des systèmes de sécurité et, d'autre part, à un accompagnement et à une sensibilisation des acteurs maritimes à la transition numérique. Sur le premier point, une uniformisation des règles à l'échelle internationale est indispensable et l'Organisation Maritime Internationale (OMI) joue ce rôle au sein de l'ONU. Son Code dresse un certain nombre de lignes directrices et contient une série de recommandations en vue d'une meilleure gestion du risque cyber. Les lignes directrices constituent la principale base règlementaire de la cyber sécurité de l'industrie maritime, et elles font l'objet d'une incorporation en droit français sous l'égide de la Direction des affaires maritimes.

Ces textes, de rang réglementaire pour la plupart, ont d'abord attribué à la Direction des affaires maritimes la responsabilité de l'approbation du plan de sûreté des navires, la délivrance, le renouvellement et le visa des certificats de sûreté des navires assujettis au code ISPS. L'approche retenue est globale : elle intègre également la gestion de menaces telles que la cybercriminalité et le terrorisme maritime. Dans ce cadre, l'évaluation doit nécessairement formaliser les mesures adoptées par la compagnie en matière de protection des systèmes de communication et d'information au niveau du plan de sûreté du navire. Ces mesures portent sur le résultat de l'évaluation, le seuil de probabilité d'accident, les systèmes clefs du navire, ainsi que les conclusions d'ordres politique et techniques relatives à la cyber sécurité du navire. Elles permettent déjà une certaine mise à niveau des capacités cyber des acteurs maritimes. Et le renforcement récent des exigences réglementaires à l'échelle européenne ne viendra que parachever cette dynamique.

En premier lieu, l'entrée en vigueur du RGPD exige une vigilance particulière des armateurs sur l'intégrité de leurs systèmes d'informations et de leur flux de données. Les compagnies maritimes sont très concernées par ce texte, au champ d'application large, en raison du caractère transnational de leurs relations commerciales qui les conduit régulièrement à contractualiser avec des acteurs européens. Par ailleurs, la définition de la « donnée personnelle » est très large et inclut certains dispositifs de la marétique.

En second lieu, la directive NIS conduit à un renforcement accru des capacités des acteurs maritimes dans la gestion du risque cyber, en ce qu'elle impose à toute entreprise nouant une relation commerciale avec l'UE de mettre en œuvre les moyens matériels, logiciels et humains nécessaires pour prévenir et atténuer l'occurrence des cyberattaques.

Cela étant, la règlementation ne fait pas tout. Si les derniers textes comportent de très fortes incitations à la prise en compte du risque cyber, ils peuvent très vite se transformer en contrainte si les acteurs ne prennent pas la mesure du changement culturel nécessaire et adaptent leurs pratiques en conséquences. Un défi demeure toujours en matière d'acculturation pour que la règlementation devienne un véritable levier de compétitivité. La transition numérique évolue d'une manière exponentielle, et surtout plus rapidement que la maitrise des nouvelles technologies. Il ne faut rien céder sur les mesures de sensibilisation aux bonnes pratiques d'hygiène numérique, sans quoi les dernières exigences risqueraient bien de manquer leur cible.

Eric Bothorel
Député
des Côtes d'Armor

2 **Vincent BOUVIER**
Secrétaire général de la mer

2 **Thibaut MARREL**
Coordonnateur sectoriel, ANSSI

3 **Bruno BENDER**
Coordinateur Cyber pour le monde maritime
Secrétariat Général de la Mer

4 **Capitaine de vaisseau BOUBÉE**
coordinateur cybersécurité, Etat-major de la marine Jusqu'en septembre 2018

5 **Stéphane MEYNET**
Président, CERTitude NUMERIQUE

6 **Vincent DENAMUR**
sous-directeur sécurité maritime direction des Affaires maritimes ministère de l'Environnement, des Transports et de la Mer

7 **François LAMBERT**
Délégué Général GICAN

8 **Lieutenant de vaisseau Olivier JACQ**
Chef de l'antenne de Brest Centre Support Cyber-défense de la Marine nationale (CSC)

9 **Franck GICQUEL**
Chargé de mission, cybermalveillance.gouv.fr

Le monde maritime est en train de vivre une révolution. La numérisation en cours du secteur est d'ores et déjà une réalité et ne cesse de s'amplifier. C'est un atout et un élément de compétitivité pour l'économie maritime, qui est aujourd'hui un secteur clé du développement commercial de la France. Mais elle l'exposera encore d'avantage à une menace cyber que la plupart des grands acteurs internationaux ont déjà affronté.

Pour mieux répondre aux enjeux de sécurité numérique de ce secteur, les organismes gouvernementaux, avec en premier lieu l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), ont mis en place un plan de défense des secteurs stratégiques dans le cadre de la loi de programmation militaire, afin de garantir la sécurité des systèmes vitaux. Avec la récente directive NIS (Network and Information Security) de l'Union Européenne, ce sont les services essentiels qui devront s'armer face au risque cyber.

D'ores et déjà, à l'occasion du Comité interministériel de la mer du 17 novembre 2017, le Gouvernement a décidé de s'appuyer sur le Comité France Maritime, placé auprès du Secrétariat général de la mer, pour structurer une filière française de la cybersécurité maritime. Le Comité France Maritime associe l'ensemble des acteurs maritimes et les régions. Sa première mission est d'effectuer un état des lieux de la filière et des acteurs maritimes de la cybersécurité. Force est de constater que les entreprises maritimes prennent en compte les enjeux de cybersécurité de façon très inégale et que de multiples structures se sont créées au fil des ans sans réelle coordination. Il est aujourd'hui indispensable d'en appréhender les rouages dans un contexte international pour en désamorcer les pièges futurs et pour en capter les opportunités.

Dans un second temps, le Comité France Maritime proposera une feuille de route avec des axes de développement pour la cybersécurité maritime. La construction de cette feuille de route associera l'ensemble des acteurs privés et publics du secteur (administrations, acteurs économiques et professionnels de la sécurité). C'est une dynamique innovante et originale dans son approche, qui doit garantir la prise en compte des spécificités du monde maritime tout en la reliant aux autres secteurs

LE DOMAINE MARITIME **SE MET EN ORDRE DE BATAILLE** FACE À LA MENACE CYBER

essentiels de notre économie. Elle doit aussi s'inscrire dans les travaux en cours de l'Union, en particulier ceux de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), des agences de classification et des assureurs. L'objectif est d'accroître la compétitivité de la place portuaire française et du pavillon français, dans un secteur fortement concurrentiel et déjà largement standardisé.

La France, dans le secteur de la cybersécurité du monde maritime, dispose aujourd'hui d'une double légitimité en tant que puissance maritime de niveau mondial et comme Nation déjà en pointe dans le domaine Cyber. Cette légitimité forte en Europe et dans le monde lui est conférée par une expertise reconnue et des savoir-faire, en particulier dans le secteur naval de défense, qui a su tirer parti des capacités d'innovation des PME de la sécurité. Cette légitimité est une force, elle nécessite d'être portée au sein des organismes européens et des instances mondiales.

Les vieux marins avaient tendance à dire que « le bien ne fait pas de bruit, et que le bruit ne fait pas forcément le bien ». C'est là, résumé, également le paradigme de la cybersécurité. Car bien plus encore qu'ailleurs, la réussite dans ce domaine expose celui qui se montre trop. Il faut pourtant porter nos savoir-faire, les exposer en cela, afin d'en tirer les bénéfices pour nos entreprises. Tant celles qui protègent que celles qui cherchent à se protéger.

Vincent BOUVIER
Secrétaire général de la mer

Le secteur du transport maritime a engagé depuis quelques années une numérisation à marche forcée. Les systèmes d'information et les réseaux informatiques ont progressivement envahi tant les ports que les navires, qui se retrouvent de plus en plus intimement connectés au cyberespace. Si cette transformation est naturellement gage de performance, d'attractivité et de croissance pour le transport maritime, dont le chiffre d'affaire global est appelé à doubler d'ici à 2050 selon l'OCDE, elle concourt à l'émergence de nouveaux risques : intrusion au sein d'un réseau, vol de données sensibles, prise de contrôle à distance de systèmes informatiques, etc.

La prise de conscience du risque cyber par les grands acteurs du secteur est d'ailleurs bien réelle. La cybersécurité fait ainsi désormais systématiquement l'objet d'interventions lors des conférences et manifestations en lien avec le maritime. Certaines organisations ont produit des guides[1] ou des projets de normes en matière de cybersécurité. Les formations aux métiers du secteur intègrent peu à peu des sensibilisations aux enjeux cyber. Enfin, en mai 2017, un chantier naval coréen majeur a livré le premier navire – un gazier – bénéficiant d'une certification cyber, délivrée par une société de classification britannique.

Cette prise de conscience a récemment été renforcée par la cyberattaque mondiale du 27 juin 2017 (généralement désignée par « cyberattaque NotPetya »), qui a gravement affecté l'activité de la compagnie danoise Maersk et provoqué une onde de choc au sein du secteur.

Au niveau français, les travaux menés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec les opérateurs d'importance vitale (OIV) du transport maritime, dans le cadre de la mise en œuvre de l'article 22 de la Loi de programmation militaire 2014-2019, ont été concrétisés par la publication en août 2016 d'un arrêté imposant l'application de 20 règles de sécurité aux systèmes d'information les plus critiques des principaux ports

LES ENJEUX DE LA RÉGLEMENTATION FRANÇAISE ET EUROPÉENNE SUR LA **CYBERSÉCURITÉ** POUR LE **TRANSPORT MARITIME**

français. La loi exige en outre des OIV qu'ils déclarent leurs incidents de cybersécurité à l'ANSSI. Deux ans après la publication de l'arrêté, force est de constater que la plupart des acteurs concernés ont désormais bien compris leur intérêt à se protéger d'une menace bien réelle et se sont mis en ordre de bataille afin de se mettre à niveau.

Au niveau européen, la directive Network and Information System Security (NIS), largement inspirée de la réglementation française sur la cybersécurité, a été adoptée en juillet 2016 par le Parlement européen et le Conseil de l'Union européenne. Sa transposition en droit français est en voie d'achèvement. Elle fournit ainsi un cadre complémentaire pour renforcer la cybersécurité du transport maritime, au-delà des seuls opérateurs d'importance vitale. Son périmètre d'application a été précisé par un décret du 23 mai 2018 et concerne de nouveaux types d'acteurs, les opérateurs de service essentiel (OSE). Ces OSE, tels que les logisticiens, les transitaires et les compagnies maritimes, fournissent un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société. Ils seront désignés par le Premier ministre et devront, à l'instar des OIV, déclarer leurs incidents de sécurité à l'ANSSI et appliquer des règles de cybersécurité, qui seront prochainement précisées par un arrêté.

Enfin, l'ANSSI se mobilise également pour la cybersécurité des navires – qui n'entrent pas dans le périmètre de ces deux réglementations – notamment au travers d'actions de sensibilisation et de conseil envers les armateurs.

CONCLUSION :

Face à une menace en forte augmentation et aux obligations réglementaires qui s'imposent à un nombre croissant d'acteurs, le monde maritime ne peut plus faire l'économie d'un engagement résolu dans la voie de la cybersécurité. Il doit pouvoir faire de cet engagement un élément stratégique et de compétitivité au niveau international.

Thibaut MARREL
Coordonnateur sectoriel, ANSSI

[1] *Voir notamment le « Guide des bonnes pratiques de sécurité informatique à bord des navires », proposé par l'ANSSI et la Direction des affaires maritimes, disponible en versions française et anglaise : www.ssi.gouv.fr/actualite/guide-des-bonnes-pratiques-de-securite-informatique-a-bord-des-navires/.*

LE MONDE MARITIME SE FÉDÈRE POUR FAIRE FACE AUX PIRATES ET CORSAIRES DU NUMÉRIQUE

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 immense 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 y circulent font l'objet de convoitises.

Milieu infini, propice à l'anonymat, le cyberespace se caractérise par sa grande similitude avec le milieu maritime. Comme lui il 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 sécurisation pleine et entière de ce milieu est une utopie. Celle des données, qui y évoluent, une nécessité sans pour autant que cette protection ne se transforme en entrave.

UNE MENACE IDENTIFIÉE.

Le monde maritime a été, très tôt, un espace d'affrontements entre nations, de façon directe ou indirecte faisant face à la présence de pirates et de corsaires, dans des zones souvent reculées. Une menace semblable se développe de façon permanente dans les profondeurs du web de façon anarchique la plupart du temps, mais parfois de façon pilotée, voire savamment orchestrée.

La cyberdélinquance est aujourd'hui susceptible de provoquer des dégâts bien plus importants sur nos économies - c'est là aussi tous les jours un peu plus vrai dans un secteur dont la numérisation va en s'accélérant.

LA SÉCURISATION DE CES ESPACES DE LIBERTÉ QUE SONT LA MER ET LE CYBERESPACE NÉCESSITE UNE ACTION GLOBALE.

Si, sur les mers, les pirates agissent de façon tradition-nelle 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. Avec la mise en place de solutions connectées de bout en bout, d'initiatives globales d'échanges d'informations dans le domaine maritime (CISE[1] en particulier) les acteurs de la filière disposeront de systèmes efficaces au service de l'efficience économique. La cyberdélinquance dans le domaine elle aussi principalement économique, cherchera à s'approprier de façon illégale une richesse à partir des données volées ou des failles exploitées en particulier sur des systèmes de bordure moins protégés et opérés par des exploitants moins organisés. La prise en compte de ces failles est importante dans un domaine qui doit s'organiser pour mettre en place les moyens permettant de répondre aux attentes des leaders bien sûr, mais aussi du tissu industriel et économique qui intervient dans le processus entier (transports terrestre, logistique, MCO,…).

DANS CE CONTEXTE, L'ÉLABORATION D'UNE POLITIQUE COORDONNÉE EN MATIÈRE DE CYBERSÉCURITÉ MARITIME DEVIENT NÉCESSAIRE.

Les professionnels de la mer et des secteurs maritimes afférents au Comité France Maritime ont exprimé le besoin que les initiatives, parfois nombreuses, mais encore éparses du domaine de la sécurité des systèmes soient structurées et adaptées au besoin. Les systèmes et les installations doivent cependant être adaptées aux contraintes du milieu et pouvoir être fédérées au sein d'une filière de cybersécurité propre au domaine. Autour du SG Mer, l'ensemble des forces vives et en tout premier lieu le GICAN, le cluster maritime et les armateurs de France se mettent aujourd'hui en ordre de bataille pour coordonner leur action et définir une stratégie pour les professionnels de la mer, par les professionnels de la sécurité.

L'action initiée en mars 2018 par le comité France Maritime et des acteurs industriels a visé à désigner un coordonnateur cyber. Il a pour mission :

- d'établir une cartographie précise des besoins ;
- d'identifier des synergies industrielles de cybersécurité pour le domaine maritime ;
- d'inscrire cette démarche dans les principales initiatives nationales, européennes et internationales.

La création d'une stratégie française structurée de cybersécurité du domaine maritime doit garantir la fiabilité des personnes, la résilience des systèmes et la protection des informations. Pour ce faire, les acteurs industriels doivent pouvoir structurer leurs réponses de façon adaptée et cohérente sur des aspects à la fois techniques, organisationnels et humains. Cette cybersécurité se doit à la fois adaptée et innovante. Pour ne pas seulement être vécue comme une contrainte, elle doit devenir une opportunité, un facteur de différenciation pour nos entreprises et pour nos ports dans une concurrence internationale de plus en plus exacerbée. Cette structuration doit s'inscrire dans le cadre des directives nationales relatives aux secteurs d'activités d'importance vitale (SAIV) et européenne des opérateurs de services essentiels (OSE aux termes de la directive NIS).

INTEROPÉRER EN TOUTE SÉCURITÉ.

Les acteurs du monde maritime évoluent aujourd'hui dans des écosystèmes complexes où l'interopérabilité est un facteur clé au service de l'efficience. Ils opèrent des systèmes toujours plus connectés, que ce soit pour le fonctionnement propre des navires et l'acheminement des biens, ou pour l'administration et la maintenance des systèmes. Considérant les orientations actuelles dans le domaine de la numérisation et la dualité de certains équipements, ces interconnections souvent « moins maîtrisées » sont appelées à se développer avec des partenaires toujours plus nombreux et parfois moins fiables. Car si le monde maritime reste avant tout un espace d'échange de biens, le monde Cyber se place au centre des données. Ces dernières sont un élément vital pour notre économie, qu'il convient de maîtriser dans leur usage au quotidien, dans l'exploitation des richesses qu'elles représentent, jusqu'à leur retrait[2], qui représentera un des enjeux futurs en particulier dans leur partage avec des tiers[3].

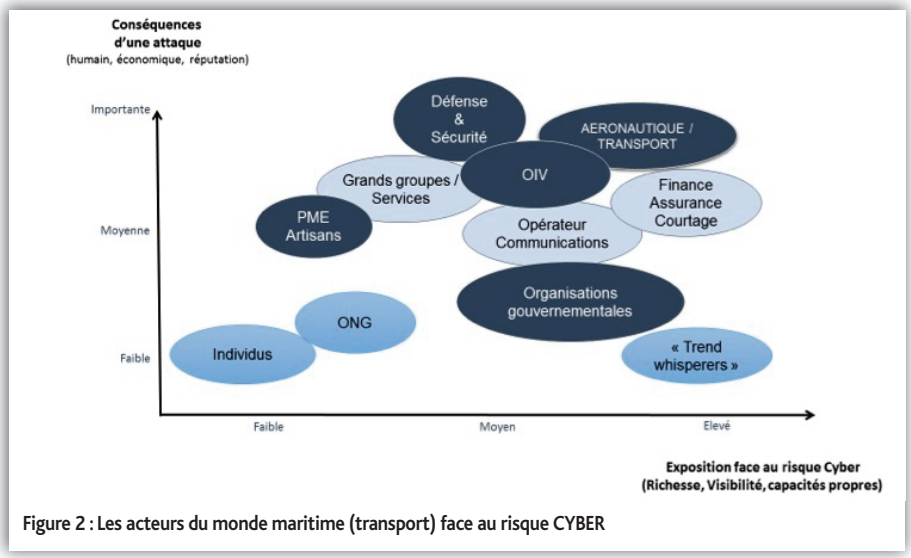


Figure 2 : Les acteurs du monde maritime (transport) face au risque CYBER

Bruno BENDER
Coordinateur Cyber pour le monde maritime
Secrétariat Général de la Mer

Bruno BENDER est un spécialiste des technologies de l'informations et de communication. Sa carrière d'officier de marine l'ont amené à servir dans le domaine des systèmes de surveillance et de communication français, européens et OTAN et d'en appréhender leur protection face à la menace Cyber. Impliqué dans la gouvernance de systèmes nationaux, UE (EUROSUR, MARSUR) et multinationaux il dispose d'une expertise dans le domaine de l'interopérabilité, et la cybersécurité des systèmes navals.

[1] *CISE : Common information Sharing environment*

[2] *NdlA : La politique environnementale de gestion des sonnées retrait des données représente un enjeu futur encore largement sous-estimé à ce jour.*

[3] *Usus : Usage de la donnée, fructus : droit de percevoir les fruits attachés à la donnée, abusus : droit de disposer de la donnée, de l'abandonner, de la détruire ou de la céder (à titre onéreux éventuellement) - « usus, fructus, abusus ».*

LE MAINTIEN EN CONDITION DE SÉCURITÉ, ENJEU MAJEUR DE RÉSILIENCE MARÉTIQUE

Le phénomène actuel de la globalisation des économies est tributaire de la maritimisation des échanges internationaux physiques et de la numérisation massive des données. A la conjonction de ces deux mondes, la marétique, cette digitalisation croissante de l'écosystème maritime, permet d'incroyables gains. Mais la révolution cybernétique que nous vivons n'est pas uniquement technique, elle induit une transformation des comportements et des usages. Le secteur maritime n'y échappe pas, il en retire un bénéfice considérable, mais en hérite une nouvelle dépendance. Cet état de fait pose en lui-même la question fondamentale de la résilience des processus et activités mis en œuvre, et du bien-fondé des organisations qui la supportent.

Les nouvelles technologies de l'information et de communication (NTIC), et donc le domaine cyber, obéissent contrairement au monde maritime et naval à des constantes de temps extrêmement courtes : pour les systèmes navals militaires, il y aura probablement cinq, six ou sept générations de télécommunication pour une génération de frégate. Ce paradoxe temps court temps long impose une stratégie de réponse comportant à la fois des mesures permanentes sur un horizon temporel lointain, des dispositions dynamiques dans l'action, et enfin être capable de s'inscrire dans la durée et de garantir la capacité à résister.

Les mesures permanentes, qu'elles soient technologiques et organisationnelles, constituent la base de la sécurité numérique : l'approche « security by design » se traduit très concrètement par un référentiel technique et réglementaire applicable à la conception des bâtiments de la marine nationale, qui comprend des exigences de cybersécurité et de sûreté de fonctionnement des logiciels.

Les mesures actives visent à anticiper, surveiller, analyser, détecter et in fine réagir face à des cyber attaques. Des systèmes de cybersurveillance scrutent les flux au cœur des systèmes, supervisés dans des « *Security Operation Center* ». Ils sont déployés et doivent être généralisés. Au-delà de ces moyens techniques, l'entraînement des forces à la cyberdéfense est essentiel car seuls les exercices permettent de confronter les hommes à la réalité, et de valider la pertinence des organisations de gestion des crises.

En troisième lieu, le maintien en condition de sécurité (MCS) vise dans le temps à maîtriser la configuration des systèmes, à les maintenir, à garantir leur intégrité, et si nécessaire à restaurer leurs capacités. Pour être pertinente et efficace, cette activité doit être menée avec une approche identique à celle de tout domaine technique non NTIC du maintien en condition opérationnelle (MCO). En d'autres termes, l'approche résiliente du MCS ne doit pas être conçue comme le MCO du domaine cyber, mais à l'inverse comme la prise en compte du fait numérique dans la totalité des aspects du MCO.

C'est un défi considérable, en raison de la complexité technique des moyens, de l'intrication des systèmes entre eux, des requalifications éventuelles à conduire, mais aussi du nombre d'industriels et d'interfaces concernés sur un navire de guerre.

Enfin, au cœur de la sécurité marétique, demeure le sujet essentiel de la ressource humaine. La compétence cyber est aujourd'hui sous forte tension, dans la société civile comme pour le monde militaire. Il faut savoir la capter, la former, la maintenir à niveau et la fidéliser. La marine s'est mise en ordre de marche pour satisfaire au mieux ses propres besoins, au travers d'un dispositif de formation adhoc.

Depuis 2014, la chaire de cyberdéfense navale à l'Ecole navale près de Brest est une brique importante de ce dispositif. Elle vise à stimuler la recherche dans ce domaine. Elle permet de développer une expertise au profit de la formation des officiers de la marine nationale, et sans doute demain du monde maritime, tout en renforçant les partenariats dans le domaine de la recherche avec les universités du grand ouest et les bureaux R&D des industriels des mondes naval et maritime.

Mais, outre la formation nécessaire de spécialistes cyber compétents et reconnus, la marine tend aussi à généraliser cette formation cyber en intégrant des modules aux autres formations à dominante technique, afin d'accompagner et maîtriser la numérisation
généralisée de ses moyens, d'en garantir l'intégrité et d'en pérenniser la sécurité.

Capitaine de vaisseau BOUBÉE
coordinateur cybersécurité, Etat-major de la marine
Jusqu'en septembre 2018

SÉCURITÉ NUMÉRIQUE DES SYSTÈMES INDUSTRIELS DANS LE DOMAINE PORTUAIRE

Les systèmes industriels, ces systèmes numériques pilotant des installations physiques, préoccupent les autorités par leurs faiblesses en matière de sécurité numérique.

Si globalement la sécurité numérique des systèmes industriels est prise en compte, parfois sous l'impulsion de réglementations nationales et européennes, il n'est pas rare de rencontrer des acteurs qui sous-estiment encore les risques ou n'accordent pas suffisamment d'importance et de moyens au sujet.

Les causes ? Le manque de formation et d'information conduisant à la méconnaissance des capacités des cybercriminels tend parfois à négliger des menaces pourtant fortement probables. La confiance « excessive » dans les systèmes et les « travers » de la culture industrielle se focalisant sur la disponibilité des systèmes écartent des scenarii d'attaques sournois visant, comme lors de l'affaire Stuxnet, à modifier le comportement des systèmes automatisés tout en leurrant les informations perçues par les utilisateurs. Enfin, le manque de connaissance des solutions existantes pour protéger et défendre les systèmes industriels conduit parfois à « repousser » les échéances.

Les systèmes industriels ont envahi nos vies à un point difficilement imaginable. Beaucoup restent persuadés de pouvoir fonctionner en l'absence de ces systèmes car, comme cela est le cas dans le milieu portuaire, des procédures existent afin de palier à une panne d'un système. Mais le problème n'est pas de pouvoir fonctionner en cas d'arrêt d'un système industriel mais de s'apercevoir, avant l'accident, que suite à une cyber-attaque, un ou plusieurs systèmes industriels ne fonctionnent plus dans leur mode nominal. Un exercice simulant ce type de scénario amènerait certainement bon nombre d'entre nous à considérer les choses sous un autre jour.

Imaginez, une station de conversion électrique aux comportements aléatoires alors que la Gestion Technique Electrique vous indique que tout va bien, ou les écluses, les ponts qui ne réagissent plus comme ils le devraient. Imaginez la détection incendie des bâtiments se déclencher de manière intempestive ou les systèmes de navigation et de signalisation fournissant des informations erronées.

Bref, le but n'est pas de citer tous les scenarii comme le ferait une analyse de risque mais d'éclairer les lecteurs sur les conséquences de cyberattaques sur les systèmes industriels portuaires.

Dans le contexte de numérisation massive de notre société, les conséquences des cyberattaques seront de plus en plus fortes, c'est une certitude. Le domaine portuaire n'échappe pas à cette règle. Si les ports sont aujourd'hui de véritables villes, de par le nombres d'acteurs, la complexité des systèmes et des réglementations, les SmartPorts de demain seront de véritables « SmartCities », devant faire face aux mêmes enjeux, aux mêmes problématiques de sécurité dont la sécurité numérique.

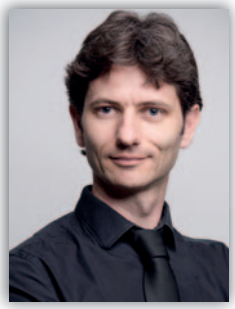
Une cyberattaque pourrait provoquer des dégâts importants, la paralysie d'un port tout entier, voire d'un territoire par effet « domino », sans compter les conséquences économiques à court terme et à moyen terme avec la perte de confiance des compagnies qui choisiront d'autres ports, qui eux, auront fait le choix d'investir dans la sécurité numérique.

Que faire face à ces menaces ? Comment (re)-donner confiance dans les systèmes numériques industriels portuaires ?

- Procédez par des actions simples, progressez par étapes et raisonner d'un point de vue de vos métiers. La sécurité numérique n'est pas un sujet d'experts techniques !
- Commencez par définir un porteur du sujet : un « pilote »
- Identifiez de manière exhaustive les systèmes industriels nécessaires au fonctionnement du port et les conséquences en cas d'indisponibilité mais aussi de perte d'intégrité, que l'origine soit une défaillance ou la malveillance d'une cyber-attaque.
- Appuyez-vous des mesures imposées pour certains opérateurs même si vous n'y êtes pas contraints.
- Envisagez l'incident et préparez-vous à le traiter. Déployez pour cela des moyens de détection, comme pour la lutte incendie, afin de réagir au plus tôt et limiter les dégâts.
- Travaillez avec toute la chaîne de sous-traitance pour que collectivement, le niveau de sécurité de vos systèmes se renforce.

Enfin, fédérer les initiatives et mutualiser les ressources ; rechercher l'efficacité et la flexibilité pour mieux connaître les menaces, les moyens de se protéger, de se défendre et mieux réagir en cas d'incident.

« Pire cauchemard » pour certains, opportunités pour les cyber-criminels, la sécurité numérique est aussi une formidable opportunité économique, ne l'oublions pas.



Stéphane MEYNET
Président, CERTitude NUMERIQUE

LES ENJEUX POUR LES ACTEURS MARITIMES DE LA RÉGLEMENTATION FRANÇAISE ET EUROPÉENNE SUR LA SÉCURITÉ NUMÉRIQUE : ...ET LES NAVIRES ?

Les directives européennes, et je ferai un focus sur la directive 2016/1148 du 6 juillet 2016 relative aux mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive NIS), imposent leur agenda aux compagnies de transport maritime.

Transposée en droit français (loi 2018-133 du 26 février 2018 et décret du 23 mai 2018) à l'instigation de l'ANSSI, la directive NIS invite la direction des affaires maritimes (DAM), en concertation avec l'organisation professionnelle « Armateurs de France », à établir la liste des « opérateurs de services essentiels » qui devront mettre en œuvre des mesures de sécurisation de leurs systèmes d'information. En fait, quatre types d'opérateurs sont concernés : outre les compagnies maritimes (services de billetterie et de réservation, enregistrement des passagers, systèmes de gestion des cargaisons de marchandises dangereuses), les opérateurs portuaires et les services de trafic maritime (certains CROSS et grands ports), et certaines entreprises de maintenance de navires.

Le constat est clair : les systèmes d'information et de supervision critiques des navires ne sont pas directement concernés. Mais est-ce une mauvaise nouvelle ?

Les navires, ces systèmes industriels isolés en mer mais désormais hyperconnectés, appellent des réglementations spécifiques qui doivent privilégier l'échelle mondiale, pour des raisons d'efficacité mais aussi de contexte concurrentiel exacerbé. L'Organisation Maritime Internationale (OMI) a ainsi publié des premières dispositions en 2016 (deux circulaires portant des premières directives de portée générale) et surtout en 2017, la Résolution MSC.428(98) qui exige la prise en compte des risques cyber dans les systèmes de gestion de la sécurité des armateurs (code ISM) selon une entrée en vigueur progressive jusqu'à 2021.

Ces textes ne représentent qu'une première étape car ils ne peuvent être considérés comme décisifs face à une menace diffuse et protéiforme. Toutefois, plus encore que pour les autres domaines, la cybersécurité des navires rend délicate l'identification du mode d'action publique le plus pertinent.

En premier lieu, compte tenu du caractère hautement technologique et évolutif de la menace cyber, les Etats se doivent de mettre en place des réglementations fondées sur l'évaluation des risques et exigeant la mise en place de processus préventifs et curatifs adaptés, plutôt que de définir un corpus de prescriptions trop détaillées.

Ainsi, au-delà de la retranscription dans le droit français de la résolution de l'OMI précitée, la DAM a initié une concertation avec le secteur, l'ANSSI et la marine nationale, afin de définir les termes d'un additif « cybersécurité » au plan de sûreté des navires qui sont dans le champ d'application du code ISPS (code international pour la sûreté des navires et des installations portuaires). Cet additif situé dans le volet curatif de la cybersécurité permettrait aux armateurs de définir à l'avance les procédures à mettre en œuvre en cas d'attaque cyber : alerte, appréhension de la portée et de l'impact, prise des mesures palliatives et de restauration des systèmes impactés.

En second lieu, les Etats ne sont que la composante supérieure d'un environnement international de sécurité maritime qui comporte des strates privées dont le rôle est déterminant. Ainsi, au regard du risque cyber, l'assurance maritime et les sociétés de classification ont vocation à jouer un rôle moteur.

A titre d'exemple, Bureau Veritas fait partie des premières sociétés de classification qui se positionnent sur le risque cyber, en publiant cette année un recueil de règles volontaires de prise en compte du risque cyber, qui s'échelonnent de la certification des registres de maintenance des logiciels à la définition d'aides à la décision. On observe également l'intensification des travaux des assureurs, avec pour objectif de proposer des polices spécifiques à la couverture d'un risque non encore pris en compte dans les polices classiques, susceptibles d'ailleurs de renvoyer à ces nouveaux modules de règlements de classe. Pour rester au niveau français, le Cluster maritime joue également son rôle en constituant un groupe de travail spécifique qui rassemble toutes les parties prenantes, privées et publiques.

Dès lors, l'administration, après les premières évaluations et publications de recueils de sensibilisation effectuées depuis fin 2015, poursuit son travail d'animation et de fédération des diverses parties prenantes. Riche d'un tissu industriel dynamique et collaboratif, la France est ainsi en capacité d'être un des pays actifs au sein des institutions internationales et européennes, sur ce sujet. Notre devoir est de poursuivre la conduite d'une analyse objective et sans cesse réajustée, sans précipitation réglementaire ni procrastination. C'est dans ce cadre que la direction des affaires maritimes examinera, au cours des prochains mois, la pertinence de définir des exigences fonctionnelles détaillées.

Et l'ensemble des parties prenantes s'accordent sur un point : il n'y aura pas de navire autonome sans une cybersécurité de haut niveau. C'est le chemin qui mène au navire autonome qui permettra les avancées les plus décisives en matière de réponse technologique, opérationnelle et réglementaire au risque cyber.

Vincent DENAMUR
sous-directeur sécurité maritime
direction des Affaires maritimes
ministère de l'Environnement, des Transports et de la Mer

LE GICAN, UN CADRE PRIVILÉGIÉ **AU SERVICE DE** LA CYBERSÉCURITÉ DU **MONDE MARITIME**

L'innovation n'est pas uniquement une idée lointaine qui viendrait assurer de la bonne santé ou de la capacité exploratoire d'un secteur dans le temps long, elle est l'assurance de sa survie à court terme au motif que, sans innovation, la préservation de la sécurité n'est pas possible. Le Groupement des industries de construction et activités navales (GICAN) a ainsi voulu s'investir dans le sujet de la cybersécurité de manière novatrice.

Le GICAN est un groupement professionnel qui rassemble les industriels français du secteur naval et maritime. Il réunit les grands maîtres d'œuvre, systémiers et équipementiers ainsi que les PME/ETI qui concourent à la conception, la construction, la maintenance et la mise en œuvre des navires militaires, des navires de commerce de moyens et grands tonnages, ainsi que des navires spécialisés, et participent à l'émergence des Energies Marines Renouvelables. Toutes les entreprises sont concernées par la cyber-menace, soit 9,5 milliards d'euros de chiffre d'affaires et 42 000 emplois directs, qui peuvent être impactés de près ou de loin.

Un gros travail de sensibilisation a été entrepris, en lien avec le CyberCercle auprès des adhérents sur le sujet et, en conformité avec ses trois missions originelles, nous devions également envisager de prendre en compte cette nouvelle menace par une innovation de trois ordres : technologique, réglementaire, de méthode.

D'abord technologique, il a fallu permettre aux Comités « Technique » et « Défense » de traiter de ces sujets. Ces deux instances du GICAN ont ainsi exprimé le souhait de travailler au mieux au développement de projets dans le domaine. Le salon Euronaval 2018 sera l'occasion d'aborder cette thématique et le GICAN souhaite notamment pouvoir mieux encadrer les start up dans le domaine naval directement intéressées au sujet de la cybersécurité. Le Seannovation devrait faire une place essentielle à ces enjeux.

Ensuite il est nécessaire de déterminer les prescriptions utiles à entreprendre auprès de l'organisation maritime internationale comme à Bruxelles dans le domaine de la cybersécurité maritime. La loi de programmation militaire avait imposé en 2013 aux opérateurs d'importance vitale des règles de sécurité et des modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité, suite à cette nouvelle législation. La Direction des Affaires Maritimes (DAM) du ministère de la transition écologique et solidaire et l'Agence Nationale de Sécurité des Systèmes d'information (ANSSI) ont publié, en septembre 2016, pour les autres opérateurs le guide « Cybersécurité, renforcer le niveau de protection du navire » mis à jour en janvier 2017.

Il reste que la capacité de prescription est trop mesurée, alors que c'est le cœur même de la guerre économique dans laquelle nous nous devons d'accompagner les entreprises françaises. Une illustration européenne, la directive NIS qui est entrée en fonction en mai 2018 impose aux Etats-membres d'adopter une stratégie nationale de sécurité des réseaux et des systèmes d'information. Les opérateurs devront sécuriser les navires, les architectures numériques et les équipements, et assurer le maintien en condition de sécurité des équipements numériques embarqués. Les entreprises françaises doivent mieux trouver leur place dans ce nouvel édifice réglementaire et c'est aussi de la responsabilité de leurs organisations professionnelles de s'organiser de la meilleure manière pour assurer la défense de leurs intérêts.

Les industriels du secteur de la cybersécurité doivent donc, ensemble, mieux connaître, notamment pour la communauté civile, les menaces spécifiques au monde maritime pour pouvoir y répondre. A ce titre, et c'est l'innovation de méthode, le Comité France Maritime nous a fait l'honneur d'accepter notre proposition de mieux s'investir dans le domaine de la cybersécurité maritime. Toute la filière maritime fait face à un grand défi et si une implication forte existe dans ce domaine, elle reste trop dispersée, des constructeurs de navires aux ports, en passant par les armateurs et les administrations. L'expertise nationale en matière de sécurité d'abord exige que cette instance devenue incontournable dans le monde maritime traite du sujet cybersécurité. En participant au financement d'un projet qui puisse permettre à l'ensemble de l'écosystème maritime de partager mieux les enjeux de cybersécurité, il a été permis d'assumer mieux cette ambition. Cette mission est celle de Bruno Bender, acteur reconnu dans la cybersécurité et qui joue ce rôle de fédérateur qui manquait au dispositif.

Les activités maritimes, industrielles, portuaires sont aujourd'hui totalement dépendantes des systèmes d'informations et de traitement des données et ainsi exposées aux cybermenaces de toutes natures. L'adaptation des navires constitue un premier enjeu et la vulnérabilité n'est pas la même selon que l'on considère l'âge de ces objets devenus connectés, sans compter les facteurs amplifiants que sont la réduction des équipages à bord des navires, l'utilisation de systèmes d'information standards, les difficultés entre le temps opérationnel et le temps informatique, le partage en temps réel des informations, les failles dans la mise en place des systèmes de détection d'attaque et de réaction à bord des navires…

Autant de défis qui attendent le syndicat professionnel de la construction navale, nous vous attendons à ce titre nombreux dans nos réunions pour coller au mieux aux préoccupations du secteur.

François LAMBERT
Délégué Général
GICAN

DEUX RÉPONSES CONCRÈTES ET EFFICACES AUX ENJEUX DE LA CYBER-MARÉTIQUE

Les enjeux de cyber-sécurité maritime sont stratégiques : la transformation numérique du secteur maritime impacte un domaine d'activité qui fait transiter 90% des marchandises échangées dans le monde. La transition progressive vers le numérique qui touche autant les navires, les armateurs que les infrastructures portuaires et *offshore* doit s'accompagner de mesures efficaces pour ne pas être vecteur de nouvelles fragilités qui pourraient le rendre vulnérable. Pour autant, le domaine est reconnu comme étant plutôt en retard en matière de cyber-sécurité. Cette relative sensation d'inertie du secteur peut s'expliquer par des normes sectorielles peu exigeantes, un déficit de prise de conscience, mais aussi par une réelle complexité de mise en œuvre des mesures organisationnelles et techniques.

En effet, les navires les plus récents sont de véritables villes flottantes : on pense au gigantisme des derniers navires de croisière, avec plus de 8 000 passagers et membres d'équipage à bord. La dimension des ports comme Marseille-Fos, Le Havre et la capacité d'embarquement de 20 000 conteneurs sur les dernières générations de navires appellent à beaucoup d'humilité quand on se penche sur leur cyber-sécurité. Assurer la cyber-sécurité d'un porte-avions comme le Charles de Gaulle, c'est sécuriser à la fois une centrale nucléaire, un aéroport et deux milles personnes, le tout projeté à des milliers de kilomètres de l'Hexagone. Un navire, ce sont des dizaines de systèmes d'informations hétérogènes, par leurs technologies, leurs fabricants et leur niveau de cybersécurité. Ce sont des systèmes isolés, interconnectés, parfois en lien avec la terre. Dès lors, par où commencer ? Quelles sont les méthodes efficaces qui ont fait leurs preuves ?

Certaines mesures ont un cycle de vie particulièrement long. Un navire construit aujourd'hui peut être exploité pendant trente voire quarante ans ! Une absence de prise en compte de la cyber-sécurité en conception a donc des conséquences à long terme qu'il est difficile de rattraper. Le RSSI doit alors apprendre à « vivre avec », oublier l'utopie du « risque zéro » et œuvrer pour réduire ces risques à un niveau acceptable. Au-delà de la stratégie indispensable mais long terme de sécurité par conception, il importe donc de réfléchir à d'autres moyens dont le bénéfice est mesurable sur le plus court terme.

Le premier vecteur d'action est l'humain. Souvent pointé (facilement) du doigt comme principale source de comportement à risques, il gagnerait à être apprécié comme un rempart efficace face au risque numérique : c'est un magnifique capteur de terrain au profit du RSSI ! Pour cela, la sensibilisation est un moyen efficace lorsqu'elle mise sur des démonstrations pratiques et des explications précises, en lieu et place des traditionnelles listes d'interdictions. L'humain doit aussi être responsabilisé dans les actions qu'il mène : l'homme joue un rôle essentiel dans la prévention des risques informatiques, par exemple pour réduire le risque d'infection viral lors d'opérations de maintenance. Ce secteur à tendance normative gagnerait à intégrer, dans le cursus du personnel navigant, ce type de formation. Mais c'est surtout l'entrainement à la cyberdéfense qui apportera un bénéfice concret en aidant à la transformation des comportements et des usages. L'entrainement régulier, en situation, du personnel, quelle que soit sa position dans l'entreprise pourra prendre plusieurs formes : de l'analyse des réactions face à du phishing à la vérification des capacités de résilience et d'autonomie à bord du navire.

Le second vecteur efficace, bien que plus complexe à mener, est la cyber-surveillance : l'analyse et la surveillance des postes informatiques et réseaux de la marétique est indispensable pour identifier à temps l'arrivée d'une menace, analyser ses impacts et mesurer les conséquences éventuelles sur l'activité métier. Le déploiement de capteurs est essentiel ; l'organisation de gestion de crise, souvent déjà existante dans le secteur, devra s'approprier le tempo des menaces cybernétiques. Mais pour être efficace, la cyber-surveillance maritime nécessitera d'une part, une action normative vigoureuse, d'autre part, un accompagnement du secteur pour mettre en œuvre ces technologies sur des systèmes complexes et enfin, une véritable organisation du secteur permettant de concevoir et d'exploiter des Security Operations Center maritimes efficaces.

Lieutenant de vaisseau Olivier JACQ
Chef de l'antenne de Brest Centre Support Cyber-défense de la Marine nationale (CSC)

Cybermalveillance.gouv.fr un partenaire pour la cybersécurité du maritime

Le dispositif national d'assistance aux victimes Cybermalveillance.gouv.fr a été lancé le 17 octobre 2017 à l'issue d'une phase d'incubation au sein de l'Agence nationale de sécurité des systèmes d'information (ANSSI) en copilotage avec le ministère de l'Intérieur et le soutien des ministères de l'Économie et des Finances, de la Justice et du secrétariat d'État chargé du Numérique.

Il est désormais piloté par le Groupement d'Intérêt Public (GIP) ACYMA.

Ses publics sont :
- les particuliers ;
- les entreprises (hors opérateurs critiques – OIV – qui relèvent de l'ANSSI) ;
- les collectivités (hors opérateurs critiques – OIV – qui relèvent de l'ANSSI).

Ses missions sont :
- l'assistance aux victimes d'actes de cybermalveillance, à travers des conseils pratiques et la mise en relation avec des spécialistes et organismes compétents proches de chez elles ;
- l'information et la sensibilisation au niveau national sur la sécurité numérique ;
- l'observation du risque numérique pour pouvoir l'anticiper.

Dans le cadre de sa mission de sensibilisation , Cybermalveillance.gouv.fr a lancé le 14 juin dernier le premier volet de son kit de sensibilisation https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/ en présence de Monsieur Mounir Mahjoubi, Secrétaire d'État chargé du Numérique et de Monsieur Guillaume Poupard, Directeur général de l'ANSSI et Président du GIP ACYMA.

Ce kit vise à sensibiliser aux questions de sécurité du numérique et à partager les bonnes pratiques. Il a été réalisé avec les membres du GIP et des utilisateurs, afin de déterminer les sujets à traiter prioritairement et les types de contenus à développer.

Une démarche originale et pragmatique a été entreprise : parler aux utilisateurs de la sécurité du numérique dans leurs usages quotidiens et privés, pour les faire progresser dans le cadre professionnel.

Cette nouvelle approche de sensibilisation permettra aux organisations publiques, privées ou associatives d'améliorer leur résilience aux risques liés au numérique, tout en développant la formation personnelle de leurs collaborateurs.

Distribués sous une licence libre (Etalab 2.0) pour en permettre la plus large diffusion, adaptation et réutilisation, les contenus de ce kit ont été pensés pour être utilisés directement, pour servir de supports à des actions de sensibilisation ou pour être intégrés à des initiatives déjà en place ou à créer.

Ce premier volet développe quatre thèmes :
- l'hameçonnage (phishing)
- la gestion des mots de passe
- la sécurisation des appareils mobiles (téléphones et tablettes)
- la sécurité des usages personnels et professionnels

Chaque thème est décliné en différents supports : vidéos, mémos, fiches pratiques et fiches « réflexe », qui s'adressent à tous quel que soit le niveau de connaissance en sécurité du numérique.

Les acteurs du monde maritime sont également ciblés par des actes de cybermalveillance : en mer comme sur terre. Les technologies modernes embarquées dans les navires, souvent connectées à internet, et l'ensemble des systèmes d'informations constituent une surface d'attaque grandissante exploitée par les cybercriminels afin de poursuivre leurs motivations, qu'elles soient lucratives, idéologiques, ludiques, pathologiques ou autre... Il est ainsi essentiel d'évaluer les risques , de se protéger en conséquence mais aussi de sensibiliser et former tous les personnels afin que l'humain soit un maillon fort du dispositif de sécurisation.

Dans cette optique, la plateforme Cybermalveillance.gouv.fr est à la disposition des acteurs du monde maritime, notamment afin de les aider dans leur nécessaire démarche de sensibilisation et d'assister les victimes en cas d'attaque.

Franck GICQUEL
Chargé de mission, cybermalveillance.gouv.fr

UN CADRE DE CONFIANCE POUR FORMER À LA SÉCURITÉ NUMÉRIQUE

Dans le prolongement de l'action qu'il mène depuis 2011 pour rendre plus appréhendables la sécurité numérique, ses enjeux, son cadre institutionnel et réglementaire, et ainsi participer à la diffusion d'une **culture cybersécurité**, le CyberCercle a créé des **modules de formation** qui permettent d'approfondir ces champs dans un cadre privilégié.

CyberCercleFormation aborde les sujets de cybersécurité dans toutes leurs dimensions et en particulier **stratégiques, juridiques et réglementaires, de gouvernance et organisationnels.**

CyberCercleFormation s'adresse à trois types de publics :

- les **dirigeants de PME-PMI** et les **cadres dirigeants non spécialistes de la cybersécurité** – directions générales, directions marketing, digital, conformité, service juridique ou ressources humaines – qui souhaitent mieux maîtriser cette nouvelle dimension indispensable aujourd'hui dans leur champ de compétences ;
- les **RSSI** et **DSI** qui désirent mieux maîtriser les **enjeux juridiques et réglementaires** liés à leurs champ d'action et responsabilités ;
- les **élus et cadres territoriaux** qui sont aujourd'hui confrontés à la transformation numérique des territoires et des usages, et qui doivent mieux appréhender la sécurité numérique pour assurer un développement pérenne de leurs actions, notamment pour garantir **la confiance dans les services numériques qu'ils mettent en oeuvre au service des citoyens.**

Les modules de formation ont volontairement des **formats courts**, d'une ou de deux journées, afin d'éviter de peser trop lourdement sur les agendas.

CyberCercleFormation propose quatre modules de formations :

- **Cybersécurité au coeur de la transformation numérique des entreprises** pour les Top managers de PME/ETI, professions libérales et activités de conseil
- **Cybersécurité au coeur de la transformation numérique des collectivités** pour les élus, directions des services généraux, directions métiers
- **Cybersécurité des systèmes industriels** pour les Top managers de PME/ETI, directions générales de service de collectivités, directions métiers, acheteurs et juristes
- **Réglementation, juridique et cybersécurité** pour les risques managers, directions de la conformité, Top managers, directions des services généraux

Les formateurs de CyberCercleFormation sont tous des **professionnels** spécialistes de la cybersécurité et dotés de qualités de pédadogue qui leur permettent de transmettre leurs savoirs de façon efficiente, en adéquation avec leur auditoire. Des **représentants des institutions publiques** viennent apporter un éclairage sur des sujets définis, permettant aux participants un accès à une expertise institutionnelle et un échange personnalisé avec les représentants de l'Etat en charge de ces questions.

En parallèle des **sessions inter-entreprises** qui seront mises en place à partir de janvier 2019 à Paris et en région, notamment en Auvergne-Rhône-Alpes et à Toulon, le CyberCercle peut définir et mettre en œuvre des formations et séminaires au sein de votre organisation, en les adaptant aux besoins et aux profils de vos collaborateurs.

cybercercle.com

UN CADRE DE CONFIANCE POUR DÉCRYPTER LES ENJEUX STRATÉGIQUES DE LA SÉCURITÉ NUMÉRIQUE

Créé en 2011, le CyberCercle est un cercle de **réflexion, d'expertise et d'échanges** sur les questions de cybersécurité, placé sous la dynamique de parlementaires et d'élus locaux, avec le soutien des institutions de l'Etat en charge de ces questions.

Plate-forme favorisant le **dialogue public-privé, cadre de confiance** à destination de l'ensemble des acteurs engagés **dans les process de transformation numérique** - entreprises, organismes publics ou collectivités - il leur permet de mieux appréhender les dimensions de sécurité numérique dans leurs projets, et de décrypter les politiques publiques, françaises et européennes.

Dans ce cadre, le CyberCercle organise depuis 2012 **des petits-déjeuners-débats mensuels** à Paris.
A partir du premier trimestre 2019, ils se dérouleront aussi à Lyon.

Le CyberCercle a également créé des **journées de rencontres à Paris, Bruxelles ou en région**, événements fédérateurs qui rassemblent les acteurs institutionnels et privés de la cybersécurité et l'écosystème sectoriel ou local concerné :

- les Rencontres Parlementaires de la Cybersécurité **#RPCyber**
- les Rencontres territoriales dans le cadre du **Tour de France de la Cybersécurité** lancé en janvier 2018 avec CCI France. En 2019, le CyberCercle sera ainsi à Bourges, Pau, Toulon, Lannion, Dijon, Lyon et Nantes.
- les Rencontres sectorielles : les Rencontres Parlementaires Cybersécurité & Milieu Maritime #RPCyberMaritime, les Rencontres Sécurité Numérique - Sécurité Portuaire (SNSP), la Conférence Cybersécurité des Collectivités Intelligentes (C3I), les SCADAYS
- l'European Cyber Day (Bruxelles).

Le CyberCercle édite également, six fois par an, une lettre d'information **« Cybersécurité et Politiques Publiques »** qui traite à chaque numéro d'un sujet déterminé, à travers des articles courts rédigés par des experts et accessibles à tous.

CYBER CERCLE

20 rue Tronchet - 69006 Lyon
contact@cybercercle.com - cybercercle.com
@CyberCercle

Réalisation impression : S.I.M. Publicité - Photo d'illustration ©bestfoto77 - Shutterstock

« DÉCRYPTER LES POLITIQUES PUBLIQUES ET DÉVELOPPER LES SYNERGIES PUBLIC-PRIVÉ EN MATIÈRE DE CYBERSÉCURITÉ POUR AGIR EFFICACEMENT ENSEMBLE »

Crédit photo : © Alain Zimeray

Cybersécurité et Politiques Publiques est éditée par le CyberCercle
Directrice de la Publication : Bénédicte Pilliet
contact@cybercercle.com

20 rue Tronchet
69006 Lyon
cybercercle.com
@CyberCercle

Les politiques publiques : un levier pour la cybersécurité

Depuis plusieurs années, la France et l'Union européenne se sont attachées à développer des politiques de cybersécurité visant d'une part, à élever le niveau global de cybersécurité des pays européens, et d'autre part, à favoriser la coopération entre ceux-ci dans le cadre notamment de la construction du marché unique numérique. L'ensemble de ces politiques publiques se doit être décrypté pour optimiser leur mise en œuvre au service, de la sécurité, du numérique et de la croissance économique.

Une lettre au service de la coopération public-privé

Dans le prolongement de l'action que le CyberCercle menons depuis 2012, nous avons ainsi souhaité renforcer notre contribution à la réflexion des grands enjeux de la sécurité numérique et des politiques publiques associées, à travers une lettre d'information portant à la fois la prise de position de politiques, élus locaux, parlementaires français ou européens, les expertises des professionnels de la cybersécurité et l'expérience des acteurs publics et privés engagés sur ces sujets.

Animé par un parti-pris éditorial original, chaque numéro de Cybersécurité et Politiques Publiques (C2SP) traite ainsi d'une thématique stratégique à travers des articles courts rédigés par un panel diversifié de rédacteurs reconnus pour leur expertise, permettant aux décideurs de mieux appréhender les grands enjeux de la cybersécurité.

Afin de permettre l'accès au plus grand nombre, CS2P est diffusée à la fois sous format papier, envoyée à une sélection de parlementaires français et européens, d'élus locaux ainsi que de représentants de l'administration et du gouvernement français, de représentants des institutions européennes et distribuée lors de nos événements. CS2P est également disponible en format électronique sur notre site.

Ce premier numéro est consacré à un sujet qui nous est cher et oh combien fondamental, sur lequel nous travaillons depuis plusieurs années, à savoir le milieu maritime. Je tiens à remercier l'ensemble des contributeurs qui ont accepté de s'associer à notre démarche. Le prochain numéro qui paraîtra en décembre traitera de la sécurité numérique et des collectivités territoriales, un enjeu d'autant plus d'actualité aujourd'hui avec la transformation numérique des territoires. Sujet d'expertise du CyberCercle, il est en particulier développé dans le cadre du Tour de France de la Cybersécurité dont chaque étape se réalise avec les villes, métropoles, communautés de communes, départements, régions qui nous accueillent.

Nous sommes bien évidemment preneurs de vos réactions et propositions dans la réalisation de ce nouveau support, que vous pouvez nous adresser via l'adresse contact@cybercercle.com.

Je vous souhaite une bonne lecture !

Bénédicte Pilliet
Présidente du CyberCercle