© DR

Didier Daoulas

© GUILLAUME GRASSET

Christophe Madec

Cybersécurité ou cyber insécurité ?

Didier Daoulas* et **Christophe Madec****
livrent leur analyse sur l'enjeu croissant de la cybersécurité, spécialement dans le monde maritime.

Propos recueillis par Denis Spilet

« La multiplication du volume des échanges de données pose clairement de nouveaux enjeux en matière de sécurité et notamment de cybersécurité. »

Didier Daoulas - Christophe Madec

M.Wang Yiwei, Directeur de *l'Institut des Affaires Internationales de l'Université du Peuple de Chine*, explique dans ce numéro de *Marine & Océans* : « *Partout dans le monde, le télétravail se répand… Sous l'effet de l'épidémie, l'intelligence artificielle se développe dans le travail à distance, le système de connexion transparente de la 5G est standardisé* ». Validez-vous ce constat ?

La crise sanitaire a, par nécessité, fortement accéléré le processus d'organisation du travail à distance pour de nombreux acteurs économiques qui n'y étaient pas tous préparés. A contrario, le monde maritime, de manière intrinsèque, a depuis toujours cette culture du travail à distance. Rappelons que 90 % du tonnage du commerce mondial est transporté par la mer et que les flux logistiques associés imposent aux organisations d'être en interconnexion permanente, et donc agiles. Il est clair que dans le « monde d'après », le déploiement de la 5G et les progrès en intelligence artificielle vont fortement participer à l'évolution des relations entre les organisations, mais aussi entre les organisations et leurs salariés. Ces évolutions vont, sans aucun doute, favoriser de nouveaux modes de collaboration. Le monde maritime nous semble parfaitement à même de s'adapter à cette nouvelle donne.

Ce contexte étant posé, quel sera l'impact en terme de sécurité de cette multiplication des transferts de données, notamment dans le monde maritime ?

Comme l'ensemble des autres secteurs économique, le monde maritime est engagé dans la révolution du digital, en rappelant qu'il s'est engagé dans la numérisation depuis plus de vingt ans. Le secteur maritime est, par définition, connecté car il met en œuvre et exploite des systèmes de navigation et de communication complexes, notamment sur la gestion du trafic maritime et des marchandises. SI l'écosystème est interconnecté, la multiplication du volume des échanges de données et les évolutions technologiques associées posent très clairement de nouveaux enjeux en matière de sécurité, et notamment de cybersécurité. Les acteurs du monde maritime sont multiples et le niveau de maturité des politiques de cybersécurité encore très hétérogènes. Ceci vaut tant pour les installations terrestres que pour les bateaux où chacun embarque et exploite un système d'information qui lui est propre. Amener au bon niveau de cybersécurité l'ensemble des acteurs du monde maritime, armateurs, installations à terres, ports, bateaux de différentes générations, constitue un véritable enjeu face au développement inquiétant de la menace cyber.

En 2016, un rapport de *la Direction des affaires maritimes*[1] évoquait l'idée d'une « cyber flotte maritime stratégique ». Il écrivait : « *A l'image de nos approvisionnements stratégiques qui imposent un quota de navires, on peut s'interroger sur le besoin pour la France de disposer d'un ensemble de navires garantissant un niveau d'exigence en matière de cybersécurité au travers d'une labellisation permettant d'assurer nos approvisionnements stratégiques* ». Qu'en est-il à ce jour ?

La France a décidé de se doter d'une véritable stratégie et de moyens d'action dans le domaine avec notamment la création, en 2019, d'un *Conseil de cybersécurité pour le monde maritime* (C2M2). Cette structure de gouvernance a pour objectif de permettre à la filière maritime d'avancer conjointement et de sécuriser sa numérisation, de la rendre cyber-résiliente. Elle agit à trois niveaux. L'analyse des risques tout d'abord : il s'agit là d'identifier les moyens d'attaque, les vulnérabilités, les conséquences potentielles. Il faut ensuite réduire la « surface d'attaque ». Cela passe, par exemple, par la formation des acteurs, la sécurisation des supports physiques des systèmes d'information, la labellisation des ports... La philosophie générale est de tirer l'ensemble des acteurs vers le haut de manière volontaire. Pour cela, une attention toute particulière est portée aux acteurs de petite taille, en leur fournissant des outils adaptés, voire un véritable « parapluie » de sécurité informatique. Enfin, il faut se donner la capacité de réagir à une attaque. C'est ce qui pousse à la création d'un *Centre national de coordination de la cybersécurité pour le maritime* (CNCCM) appuyé sur une *Cyber Emergency Response Team* du secteur maritime (CERT-M) qui apportera une véritable capacité d'action en cas d'attaque. *L'Agence nationale de sécurité des systèmes d'information* (ANSII) est un acteur-clé de ce processus, même si les acteurs du secteur maritime y participent également activement au sein du C2M2.

« Amener au bon niveau de cybersécurité l'ensemble des acteurs du monde maritime constitue un véritable enjeu face au développement inquiétant de la menace. »

Didier Daoulas - Christophe Madec

© DR

*Expert en sécurité maritime, sécurité nucléaire, et cybersécurité, ancien commandant de la base opérationnelle de l'Ile Longue à Brest, base des sous-marins nucléaires lanceurs d'engins (SNLE) de la Force océanique stratégique française.

**Directeur de clientèle, Expert Cyber & Fraude chez BESSÉ Industrie & Services, fort de plus de vingt ans d'expérience au sein de diverses compagnies d'assurances et courtiers de premier plan. Expert *Lignes Financières et Transfert Alternatif de Risques*. En charge des solutions innovantes contre les risques Fraude et Cyber.

1 - Ministère de l'environnement, de l'énergie et de la mer – Cybersécurité, évaluer et protéger le navire - septembre 2016