ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 14279	De **M. Didier Le Gac** (Renaissance - Finistère)	**Question écrite**
Ministère interrogé > Mer	**Ministère attributaire** > Mer et biodiversité	
Rubrique >mer et littoral	**Tête d'analyse** >Situation de France Cyber Maritime	**Analyse** > Situation de France Cyber Maritime.
Question publiée au JO le : **09/01/2024** Date de changement d'attribution : **02/04/2024** Date de renouvellement : **16/04/2024** Question retirée le : **11/06/2024** (fin de mandat)		

Texte de la question

M. Didier Le Gac attire l'attention de M. le secrétaire d'État auprès de la Première ministre, chargé de la mer, sur l'augmentation préoccupante des cyberattaques dans le domaine maritime et portuaire au niveau mondial et sur la capacité de la France à y répondre, notamment en renforçant les capacités de France Cyber Maritime. Engagés dans une transformation numérique profonde afin de gagner en performances et compétitivité, les secteurs maritimes et portuaires français sont aujourd'hui intégrés et interconnectés à de nombreux systèmes et bases de données assurant et optimisant le fonctionnement d'équipements industriels, de gestion de flux logistiques, de moyens de communication, de régulation du trafic ou de sécurité maritime. Néanmoins cette intégration et cette dépendance croissante au numérique augmente la vulnérabilité aux cyberattaques. Ainsi, par exemple, en juin 2017, la compagnie danoise Maersk est victime d'une cyberattaque qui neutralise en sept minutes 4 000 serveurs et 45 000 ordinateurs de l'entreprise à travers le monde, avec pour conséquence l'arrêt de 20 % de la capacité mondiale du transport maritime et le blocage de millions de conteneurs non identifiés sur les terminaux portuaires faute d'accès aux serveurs. Le coût de cette attaque pour la compagnie est estimé à 300 millions de dollars. Dans un tel contexte marqué par la forte dépendance du commerce extérieur du pays au transport maritime à hauteur de 70 %, la France s'est engagée avec les administrations et services de l'État concernés (SGMer, DGAMPA, DGITM, ANSSI) à intégrer la cybersécurité maritime dans sa stratégie nationale de sûreté maritime et portuaire. À la suite du Conseil interministériel de la mer de 2018 (CIMer), le Conseil de la cybersécurité du monde maritime (C2M2) est chargé de définir la stratégie et d'orienter les actions des acteurs publics et privés concernés par ces risques impactant directement la souveraineté nationale. La mesure 46 du CIMer de 2018 confirme ainsi que « la France prend toute la mesure des enjeux liés à la cybersécurité dans le domaine maritime, à la fois en matière de protection des systèmes d'information et en matière de développement économique (...) et décide ainsi la création d'une commission cybersécurité et la préfiguration d'un centre national de coordination de la cybersécurité pour le maritime ». Afin d'atteindre ces objectifs, France Cyber Maritime est créée en novembre 2020 sous forme d'association avec pour mission de contribuer directement au renforcement de la cybersécurité du secteur maritime et portuaire français, dans un contexte de numérisation accrue des navires et des ports nationaux et de l'augmentation des menaces cyber. L'instruction interministérielle n° 230/SGDSN/PSE/PSN/NP du 28 juin 2022 relative à l'organisation et à la coordination de la sûreté maritime et portuaire précise ensuite que pour faire face aux attaques dans le domaine numérique (...), « France Cyber Maritime a pour mission de renforcer la résilience du secteur maritime et portuaire. Elle est plus particulièrement chargée de mettre en œuvre, à terme, le *Maritime Computer Emergency Response Team* (M-CERT), centre de veille, d'analyse, d'alerte et de recueil des incidents cyber avec l'appui de l'ANSSI (...) ». Ainsi, depuis sa création, France Cyber Maritime, en lien avec l'État et en

soutien de la stratégie nationale de cybersécurité maritime, met en œuvre le M-CERT aux fonctions comparables à un centre régional opérationnel de surveillance et de sauvetage (CROSS) pour le cyberespace maritime et fournit régulièrement informations, alertes et assistances aux acteurs du secteur, notamment en cas de cyberattaque. Aujourd'hui reconnue internationalement par l'Agence européenne pour la sécurité maritime (EMSA), la direction générale des affaires maritimes et de la pêche de la Commission européenne (DG MARE) et l'OTAN, France Cyber Maritime doit poursuivre sa montée en puissance et pérenniser ses ressources pour répondre aux besoins croissants du secteur maritime et portuaire français. Néanmoins, son modèle de financement basé sur les cotisations de ses membres, les subventions de collectivités et une subvention du secrétariat général de la mer (SGMer) avec le soutien de l'Association nationale de la sécurité des systèmes d'information (ANSSI) dans le cadre du volet cybersécurité de France Relance (1 million d'euros sur 3 ans de 2021 à 2023), destinée exclusivement au démarrage du M-CERT, ne permet plus d'assurer une réponse performante au-delà de 2024, ni le maintien et le recrutement de collaborateurs indispensables aux missions qui lui sont attribuées. C'est pourquoi il lui demande quelles mesures le Gouvernement entend prendre pour pérenniser le financement de France Cyber Maritime et, ainsi, assurer le développement d'une politique nationale indépendante et souveraine de prévention et de lutte contre les cyberattaques du secteur maritime français à la hauteur des enjeux porté par l'État, dans un contexte international de plus en plus propice à la cybercriminalité de toute nature.