BREVES MARINES N°271

LA MER, TERRITOIRE DE CONFRONTATION CYBER

Davantage numérisé, toujours plus connecté, le monde maritime est particulièrement vulnérable face aux risques cyber, leurs conséquences pourraient être désastreuses. L'emploi du cyber dépasse le seul secteur militaire et s'étend à l'activité maritime dans son ensemble, au point de parler de « marétique ». Le cyber recouvre aussi un nouvel espace qui s'intègre pleinement dans l'architecture de la stratégie navale.

LES ESPACES CYBER ET MARIN : DES MILIEUX COMMUNS ET INTERDÉPENDANTS

Les espaces cyber et marins partagent un certain nombre de points communs. Ils sont au cœur des échanges internationaux (commerciaux, financiers, d'informations, etc.) et sont caractérisés par l'immensité de leur territoire, aux frontières non tangibles, qu'il est difficile de contrôler en permanence. La notion de liberté de navigation, au sens propre comme au sens figuré, est également partagée au sein de ces deux espaces.

Tout en étant similaires, ces espaces sont aussi interdépendants. Les câbles sous-marins constituent un élément essentiel pour la circulation de l'information tandis que le monde maritime est également fortement numérisé.

LES CÂBLES SOUS-MARINS : UNE TECHNOLOGIE ESSENTIELLE POUR LE TRANSIT DES COMMUNICATIONS

Aujourd'hui, plus de 400 câbles sous-marins reposent au fond des océans, assurant 99% du transit des télécommunications (dont notamment les données relatives aux opérations financières, militaires, et au renseignement). Infrastructures fragiles, mais vitales, ils représentent la couche physique du cyberespace, dont la protection est stratégique.

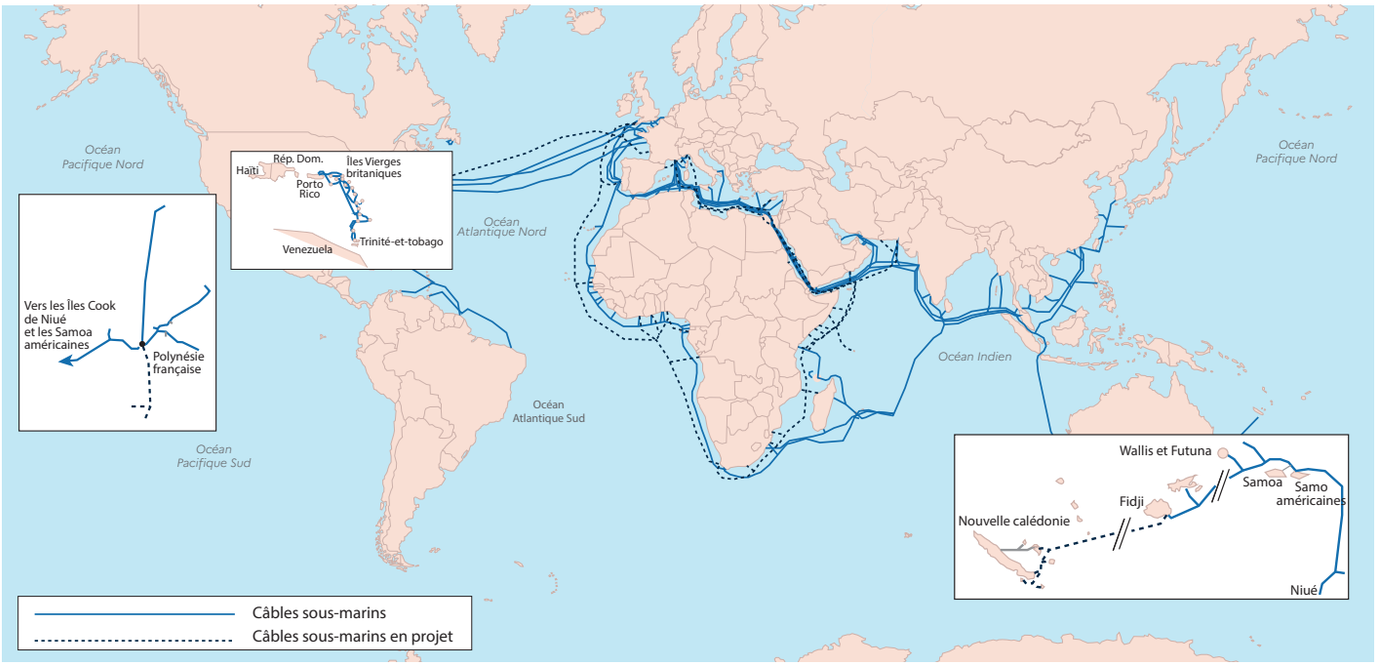
LES VULNÉRABILITES DE L'ESPACE MARITIME

Dans un contexte de maritimisation, l'économie mondiale dépend aujourd'hui majoritairement des mers et océans : 90% des échanges mondiaux sont assurés par le transport maritime. Or, la bonne conduite de ces activités repose sur la circulation sécurisée des flux d'informations, dont la manipulation ou l'exploitation malveillante constitue une menace bien réelle.

En effet, la capacité de contrôler un pétrolier, de fermer un port, de divulguer la position confidentielle d'un navire sont des risques à envisager. Une cyberattaque, même mineure, peut entraîner des pertes financières importantes. De plus, la massification du transport maritime a amené le secteur à se numériser dans tous ses aspects. L'informatisation et l'autonomisation généralisées des systèmes de l'activité maritime – dite marétique – permet d'augmenter la productivité du secteur. Le développement rapide de nouvelles technologies performantes pour la navigation, la communication et la logistique génère une dépendance croissante du milieu maritime à l'électronique à bord, à l'informatisation des systèmes ou à la mise en réseaux des ports et des navires.

En corollaire, le secteur recense un nombre croissant de cyberattaques (+400% d'attaques ciblant l'économie bleue au premier semestre 2020). Construction navale, ports, transport maritime, plateformes pétrolières ou activités de croisière sont les principaux secteurs visés.

LES PRINCIPAUX CÂBLES SOUS-MARINS DE COMMUNICATIONS DANS LE MONDE



Avec l'interconnexion de la filière maritime, une cyberattaque sur l'un des secteurs a des conséquences sur l'ensemble du domaine. Par exemple, en juin 2017 l'armateur Maersk a été victime du ver informatique *NotPetya*. Impactés, les ports de Rotterdam, New York, Mumbai et Buenos Aires ont été contraints de fermer, soit une perte de 300 millions de dollars.

L'ENJEU STRATÉGIQUE DU CYBER

Dans le domaine maritime, les cyber-menaces touchent indifféremment les secteurs civil et militaire. Ceux-ci partagent en effet des vulnérabilités semblables : par exemple, la manipulation du système de navigation d'un navire militaire pour le dérouter dans un détroit ou en direction des eaux territoriales d'un État.

Les navires de guerre disposent de systèmes spécifiques pour assurer la conduite des opérations. Un bâtiment militaire est également un ensemble de systèmes opérationnels, utilisés pour l'identification, le positionnement (AIS), la navigation (RADAR, GPS) mais inclut aussi des systèmes d'armes et des outils d'échange d'informations tactiques. L'échange effectif des données est ainsi au cœur des opérations navales, et leur protection constitue un enjeu stratégique. Dans le domaine militaire, la principale menace cyber est invisible : il s'agit de l'espionnage et du recueil de l'information stratégique. Si les navires militaires constituent des cibles encore plus sensibles, de par la confidentialité et l'intérêt tactique ou stratégique de leurs activités, la problématique cyber est désormais pleinement intégrée au domaine militaire. Les constructeurs navals jouent là un rôle majeur, puisqu'ils doivent intégrer des systèmes numériques complexes, et sécurisés, à bord des nouveaux bâtiments, tels que les FREMM ou les FDI. C'est donc tout l'écosystème du navire qui doit être sécurisé.

LA MARINE NATIONALE : ACTEUR DE LA CYBERDÉFENSE

Aujourd'hui pleinement consciente des enjeux du cyber, la Marine a créé une unité spécifique et opérationnelle à la pointe de la lutte informatique : le Centre support cyberdéfense (CSC), basé à Toulon et à Brest. Le CSC assure une cyber-surveillance de l'ensemble de l'écosystème Marine nationale, et est capable d'intervenir rapidement en cas d'incident. L'objectif est d'assurer un maximum d'autonomie à la mer, en protégeant la connectivité des navires. Dans un contexte d'augmentation globale des cyber-attaques, de plus en plus d'incidents sont enregistrés aujourd'hui, mais les impacts opérationnels sont moindres, grâce à une meilleure efficacité dans la lutte.

Milieu d'opportunités et de menaces, le cyberespace ouvre un nouveau champ d'action pour la Marine. En 2021, l'exercice Polaris21 a ainsi intégré des scenarii dans le cyberespace. Alors que l'horizon du cyberespace se mêle à celui de la mer, les forces navales françaises déploient aujourd'hui d'importants moyens pour maitriser leur environnement numérique et assurer les opérations navales dans un espace toujours plus complexe.

LA MENACE CYBER DANS LE DOMAINE MARITIME