# La marétique, un enjeu essentiel pour l'humanité ?

***Florian MANET***
*Colonel de la Gendarmerie nationale*
*Commandant la SR de Bretagne*
*Essayiste*

***La marétique interroge sur la pleine maîtrise par l'homme de cet écosystème numérique complexe. Le capitaine est-il encore maître de son propre navire tant l'internet industriel prospère à bord ?***

Le 28 septembre 2020, la CMA-CGM a reconnu avoir été victime d'un rançongiciel, précédant, symboliquement, de quelques jours, l'Organisation Maritime Internationale. En septembre 2018, les ports de Barcelone et de San Diego en Floride ont aussi été perturbés par une cyberattaque. Ainsi, ces exemples illustrent l'actualité de la cybersécurité affectant les acteurs maritimes. 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 à l'informatique, « désigne l'ensemble des systèmes informatique et électroniques utilisés dans la gestion et l'automatisation des activités maritimes, fluviales et portuaires »[1]. La numérisation irrésistible de l'espace maritime accompagne la maritimisation des échanges physiques comme immatériels. 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 ?

Ainsi, l'écosystème numérique maritime aiguise les appétits d'organisations criminelles internationales en recherche de profits et de visibilité politiques pour des mouvements terroristes. La prise en otage de données et de services nourrit un capitalisme criminel très prospère. Au total, une marétique sécure apparaît comme le garant de la résilience de la globalisation et des équilibres interétatiques.

## Entre la thalassocratie maritime[2] et les terroristes, les acteurs de la marétique : la marétique, ultime révolution maritime ?

La révolution de la marétique au tournant des années 2000 est comparable à l'apparition du gouvernail ou du GPS. Désormais, le navire est pleinement intégré dans

[1] *Livre bleu sur la marétique*, 2013

[2] *Le crime en bleu, essai de thalassopolitique,* Florian MANET, édition NUVIS, 2018

une bulle technologique mondiale qui amarre ce vecteur, jadis totalement indépendant, à un écosystème complexe, celui d'une chaîne logistique mondiale interconnectée.

L'univers mental du marin est aussi bouleversé. Outre les aléas naturels, le suivi mécanique ou l'attention portée aux obstacles à la navigation, il doit désormais intégrer les liaisons numériques. Immatérielle et invisible, cette menace pose problème dans sa prise en compte, car elle est trop souvent résumée à un sujet de sécurité informatique, pré carré de quelques experts.

D'ailleurs, le cadre légal et réglementaire propre au maritime paraît timide sur l'internet des objets et, plus largement, l'internet industriel en comparaison avec d'autres sujets de sécurité maritime (sauvegarde de la vie humaine, pollution maritime).

La marétique est d'autant plus fondamentale que la communauté maritimo-portuaire a tous les atouts pour séduire les cybercriminels. Internationale par construction, l'économie bleue rassemble de très nombreux maillons, certes physiquement distants, mais unis par le digital. Ainsi, l'affrètement d'un conteneur de 20 ou 40 équivalent vingt pieds impose l'échange d'une masse conséquente de données entre au moins une vingtaine d'opérateurs. Sans compter les transactions financières.

## La thalassocratie criminelle ou la maritimisation de la criminalité organisée

Les activités maritimes sont une caisse de résonance internationale et une source de profits exceptionnels pour des acteurs malveillants. Ils 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 est uniquement mue par l'appât du gain, les deux autres agissent par idéologie et par volonté déstabilisatrice d'une organisation étatique.

Le cyber-malfaiteur est nommé hacker ou pirate. L'analogie avec le monde maritime est riche de sens. Agissant hors des eaux territoriales et hors de toute revendication politique, il illustre le rapport inversé du faible au fort, ce que rend possible le milieu maritime et … le numérique. Un semi-rigide armé par un groupe de pirates peut 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 grecques 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 ».

Le nombre de pirates est aussi incertain que celui des attaques perpétrées sur les réseaux et le gain réalisé. L'analyste bute sur un chiffre noir[3] qui dissimule une réalité en expansion.

## Un capitalisme criminel se nourrissant de la maritimisation

### Un *business model* fondé sur la valeur ajoutée de la data et du service

Au sein du « capitalisme criminel », ce système économique « gris », tout s'échange et s'achète. Compétences, services, données. À l'image de l'économie réelle, des prestataires (codeurs, hébergeurs, call-center, webdesigner, financiers…) offrent leur service sur le darkweb à des entrepreneurs criminels.

[3] Désigne l'ensemble des crimes qui ne sont pas connus du système pénal et qui échappe à l'investigation et à une réponse pénale faute d'une plainte.

Le paiement de la rançon 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. Très opportunistes, ces organisations exploitent une faiblesse dans le dispositif de sécurité numérique. 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.

## L'IT et/ ou l'OT au cœur d'une stratégie malveillante

Que les motivations soient criminelles ou politiques, la manière d'opérer consiste toujours à pénétrer, par ruse, effraction ou escalade, les systèmes d'information (IT) ou d'exploitation (OT). Insidieux et discret, le pirate dépose dans un premier temps, une infection sur un système, puis, met en œuvre ses effets (chiffrer, aspirer, contaminer, maîtriser la production d'un service) et, enfin, signe son méfait.

Les cyberattaques sur les acteurs maritimes témoignent d'une grande diversité visant à la fois l'IT (réseaux on shore de l'armement CMA CGM le 28 septembre 2020 ou l'opérateur portuaire MAERSK cible du rançongiciel Not Petya le 27 juin 2017) tout comme les OT (prise de contrôle à distance des fonctions essentielles à la navigation ou au système portuaire, émission d'informations fausses de positionnement…). Ses effets perturbent les opérations à la mer comme à terre, affectant les flottilles comme les infrastructures logistiques.

## La marétique, garant d'une globalisation résiliente et de la stabilité internationale ?

### Un risque majeur pour la navigation maritime

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, les prises de contrôle à distance de fonctions essentielles à la navigation génèrent des événements de mer (collision, talonnage, avarie mécanique…) dont les conséquences sont irrémédiables sur l'écosystème maritime (rejet d'hydrocarbures) ou sur la navigation (obstacle à la navigation). La mer amplifie systématiquement les conséquences, dans l'espace comme dans le temps.

Qu'en est-il de l'établissement des responsabilités ? Bien souvent, la réussite d'une cyberattaque repose sur une faute humaine. Même si -admettons le- le hacker agit par ruse ou tromperie, rendant la détection du stratagème très complexe. La marétique interroge sur la pleine maîtrise par l'homme de cet écosystème complexe. Le capitaine est-il encore maître de son propre navire tant l'internet industriel prospère à bord ? Ainsi, émerge, dans le brouillard d'une digitalisation galopante et dans le spectre potentiel du navire autonome ou 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 vecteur de 90 % du commerce constitue le centre de gravité des chaînes logistiques mondiales. Les projets de port connecté ou intelligent ou smart port, conditionnent, en effet, la fluidité des dynamiques d'approvisionnement terrestre en amont comme en aval du navire. Sécuriser l'expédition maritime, c'est donc contribuer à garantir la régularité des approvisionnements d'économies fonctionnant à flux tendus ; c'est fiabiliser l'activité portuaire et l'exploitation des espaces maritimes. C'est in fine contribuer 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 ?

***Les opinions exprimées ci-après sont celles de son auteur. Elles n'engagent aucunement la Gendarmerie nationale.***