Le jour de la Cybersécurité maritime

	Le jour de la Cybersécurité maritime

---

Alors qu'était publié le 25 décembre 2011 mon premier article consacré à (l'absence de) la cybersécurité dans le secteur maritime, jamais je n'aurais imaginé y revenir avec une telle régularité chaque 25 décembre depuis [1].

De là à imaginer que ce jour pourrait devenir LE jour de l'année où l'on y penserait, il n'y a qu'un pas que j'ai eu envie de franchir ! J'appelle donc solennellement de mes vœux, et en toute simplicité, qu'une autorité nationale, européenne voire internationale décrète que chaque 25 décembre soit la journée de la cybersécurité du secteur maritime.
Si mon souhait se perd dans l'immensité intersidérale du cyberespace, vous pouvez compter sur moi pour cette amicale « piqûre de rappel » aussi longtemps qu'elle sera nécessaire. En souhaitant simplement que je cesse ce rappel avant 2020 sinon cela signifiera que le niveau d'inquiétude et, surtout, de risque aura grimpé en flèche. Mais puisque c'est actuellement la trêve des confiseurs et parce que l'année 2015 aura été particulièrement difficile en France [2], essayons de rêver quelques instants.
Saluons tout d'abord la tenue des « premières rencontres parlementaires cybersécurité et milieu maritime » le 12 février 2015 à Paris, brillamment organisées par le « Cybercercle » qu'il convient ici de saluer pour son rôle et son activisme passionné. A la suite de cette journée, une lettre autour de ces rencontres, que je recommande, a été publiée [3].
Fin octobre, le colloque Safer Seas [4] a réuni à Brest l'ensemble des acteurs du secteur. Une part modeste mais somme toute bien visible [5] a été laissée à la cybersécurité notamment sous l'angle de la cybercriminalité [6].
Si, sans doute, trop nombreux sont encore les décideurs du secteur maritime à découvrir que des ports aux navires en passant par la supply chain tout ce qui embarque de l'informatique doit être soumis à interrogation, ne boudons cependant pas notre plaisir. Oui la prise de conscience a lieu et, oui, enfin, tout le monde est en train de (ou va prochainement) se mettre autour de la table pour en discuter.
La prochaine étape va donc consister à passer de la prise de conscience aux paroles, que l'on espère fortes, puis à leur concrétisation : évaluation globale des risques informatiques, audits [7], développement et insertion de services et de produits qualifiés [8], processus d'homologation [9], éducation via de la sensibilisation à l'ensemble des salariés de la filière, bonnes pratiques, etc. L'ampleur de la tâche étant si vaste [10], il faut simplement souhaiter et agir rapidement pour que les prochaines étapes ne s'effectuent pas au rythme d'une annexe à rame mais bien plus sur celui d'un hydroglisseur commandé par un capitaine expérimenté et volontaire, entouré d'un équipage adroit et tenace y compris – et surtout – au cœur des tempêtes qui s'annoncent.

[1] ou presque : 2013 puis 2014
[2] tant par les attentats de janvier et de novembre que par l'inexorable montée du chômage et la paupérisation continue d'une part croissante de nos concitoyens
[3] http://fr.calameo.com/read/004370735c23949b43ff3
[4] http://www.saferseas-brest.org/
[5] http://presse.rivacom.fr/fr/newsletter/1494/la-cybersecurite-un-enjeu-majeur-pour-le-monde-maritime
[6] http://www.letelegramme.fr/bretagne/mer/cybercriminalite-bateaux-et-ports-pour-cibles-28-10-2015-10829564.php
[7] http://si-vis.blogspot.fr/2015/02/tester-son-niveau-de-cybersecurite.html
[8] http://www.ssi.gouv.fr/entreprise/qualifications/
[9] http://www.ssi.gouv.fr/actualite/pour-homologuer-votre-systeme-dinformation-suivez-le-guide/
[1 0]
http://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-recorders-vulnerable-to-attack/

Réagissez à cet article

Source : *Si vis pacem para bellum: Cybersécurité maritime 2015*