



MINISTÈRE DE
L'ENVIRONNEMENT, DE
L'ÉNERGIE ET DE LA MER

DGITM

Direction des Affaires Maritimes

- CYBER SECURITE - renforcer le niveau de protection du navire

Pour aller plus loin :

www.ssi.gouv.fr

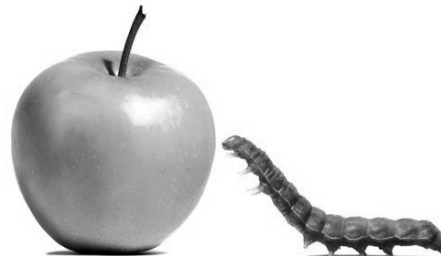


Objectif principal :

*Sensibiliser les compagnies
maritimes aux cybers menaces à
bord du navire.*

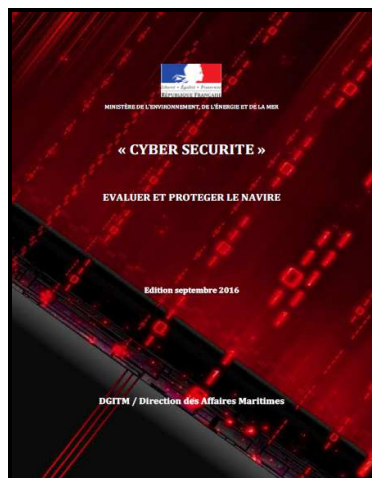
Des vulnérabilités ...

- La vulnérabilité des systèmes embarqués et la dépendance du navire à ces systèmes,
- L'inter connectivité des systèmes d'information à bord du navire et vers l'extérieur,
- Le développement des moyens nomade,
- La non mise en œuvre de plan de sécurité de l'information et de plan de continuité d'activité à bord du navire,
- Le manque de formation de l'équipage pour évaluer un acte de malveillance.



... Des risques

- La dégradation de l'image de la compagnie pouvant aboutir à une perte de compétitivité de la compagnie,
- Le sabotage du navire par système dormant ou opéré sur demande pouvant aboutir à la perte du navire, la perte de l'équipage ou l'atteinte à l'environnement.

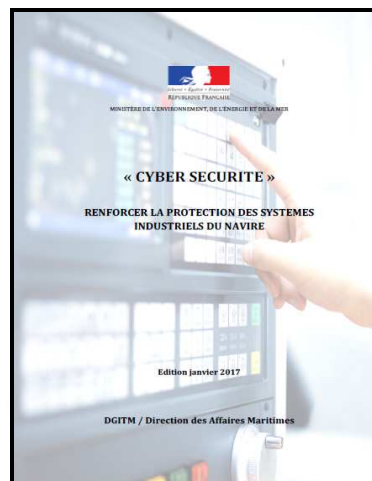


Outil n°1

(Une enquête + un audit = 7 fiches de recommandations)

Ce document issue d'une enquête conduite par la DAM et d'un audit navire conduit par l'ANSSI décrit les mesures à mettre en œuvre afin d'élever le niveau de protection du navire :

- R1 / Confiance numérique du navire.
- R2 / Gouvernance.
- R3 / Gestion des accès et des fuites de données.
- R4 / Sécurisation des transactions,
- R5 / Continuité de service,
- R6/ Traçabilité et audit,
- R7 / Confidentialité.

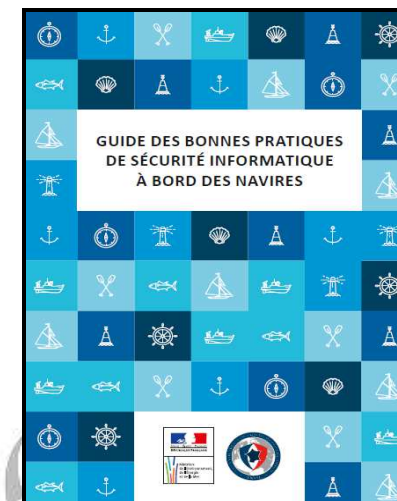


Outil n°2

(Une analyse de risques)

Faisant suite à l'évaluation des risques issue du document n°1, cette analyse illustre les moyens pouvant être mis en place pour protéger les systèmes industriels embarqués à bord du navire :

- N1 / Stratégie globale de sécurisation,
- N1 / Maitrise de l'internet des objets,
- N2 / Surveillance passive,
- N3 / Durcir la chaine de contrôle des systèmes industriels.



Outil n°3

(Prendre en compte l'élément humain)

Ce dernier outil vise à sensibiliser le marin et la compagnie pour mieux appréhender le cyber risque :

- **Choix du mot de passe,**
- **L'utilisation de la messagerie,**
- **Séparer les usages,**
- **Etre prudent sur internet,**
- **Téléchargement, sauvegarde, Wifi...**

WEBSITE : <http://www.developpement-durable.gouv.fr/surete-des-navires-et-surete-portuaire>