PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la mer

BESSÉ
CONSEIL EN ASSURANCES

RAPPORT D'ANALYSE DE RISQUES CYBER DES SECTEURS MARITIMES ET PORTUAIRES

SYNTHÈSE

Comité analyse des risques du Conseil de Cybersécurité du Monde Maritime (C2M2)

DÉCEMBRE 21

LE SECTEUR MARITIME ET PORTUAIRE FACE AU RISQUE CYBER

Denis ROBIN
Secrétaire général de la Mer

Comme l'ensemble du monde, le secteur maritime et portuaire est entré dans l'ère du numérique : les systèmes et sous-systèmes des navires et des ports sont de plus en plus pilotés numériquement et interconnectés même lorsque les navires sont en pleine mer. Cette évolution, indispensable car gage d'efficacité, a exposé le monde maritime et portuaire à un risque qui ne le concernait jusqu'alors qu'assez peu : le risque cyber.

Le domaine maritime et portuaire est particulièrement exposé aux attaquants cyber du fait de l'importance des flux financiers qu'il génère

Face à ces menaces élevées, le secteur maritime et portuaire s'est organisé, en créant notamment le Conseil Cyber du Monde Maritime (C2M2), dont les travaux ont suivi deux orientations. La première est l'analyse détaillée des risques et des scénarios d'attaques possibles, objet de ce rapport. Cette identification des vulnérabilités permet de prioriser les actions à mener. La seconde est l'adoption d'une stratégie cyber du monde maritime, identifiant lesdites actions. Elle s'est concrétisée par la création de l'association France Cyber Maritime, dont la vocation est d'étendre au domaine cyber le principe de solidarité des gens de mer qui fait la force du monde maritime.

Le risque cyber ne disparaîtra pas. Mais avec les efforts de tous, ce risque sera maîtrisé, comme le monde maritime et portuaire a toujours su le faire pour les nombreux autres risques auxquels il est exposé.

Didier DAOULAS
Directeur du comité « Analyse des risques »
Ingénieur département Maritime - Bessé

L'analyse a été menée pendant 6 mois de manière méthodique en s'appuyant sur la connaissance de l'écosystème maritime français, en recensant les évènements redoutés par domaine d'activités tout en s'attachant à rester macroscopique afin d'en tirer les enseignements majeurs pour le secteur. Elle intègre l'état de la menace et les sources de risques connus, elle tient compte également des avis des compagnies maritimes et des ports que nous avons pu consulter. Par construction, elle met l'accent sur les vulnérabilités plutôt que sur les forces afin d'identifier et retenir les scénarios dont l'impact serait significatif sur le secteur. Ceci n'occulte en rien le travail de qualité réalisé par tous les acteurs au quotidien mais permet d'alimenter la réflexion et de proposer des axes d'amélioration et des recommandations d'ordre organisationnel, technique ou réglementaire.

Ce rapport s'adresse à tous ceux au sein des secteurs maritimes et portuaires français et parmi leurs partenaires clés qui contribuent à la sécurité informatique et qui, conscients du risque, la font progresser par leurs actions. Elle a également vocation à être prise en compte par le comité « prospective et régulation » en charge de développer une stratégie de cyber sécurité ainsi que par l'association France Cyber Maritime, dont je remercie l'implication et le soutien.

OBJECTIF

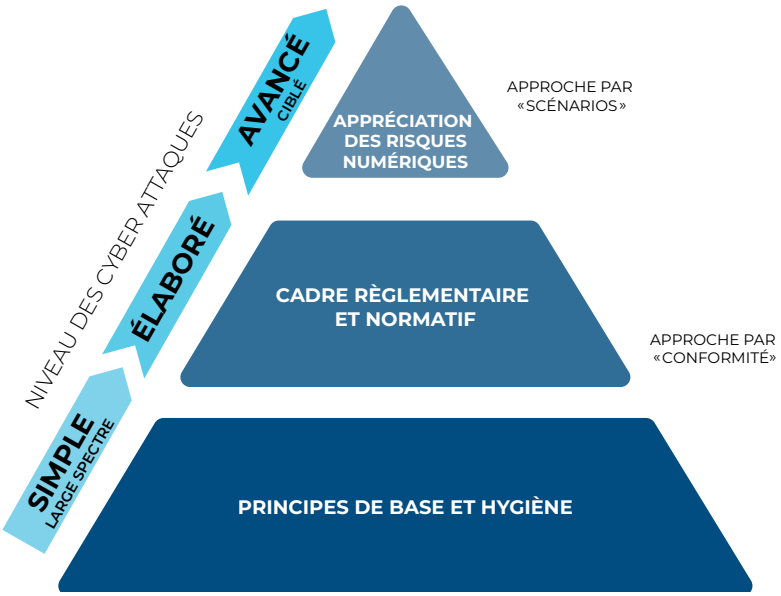
L'objectif de cette étude est de réaliser une analyse de risques macroscopique du secteur maritime français vis-à-vis de la menace cyber. Il s'agit d'identifier les risques les plus significatifs pour le secteur maritime et portuaire français et de proposer des recommandations pour les réduire.

MÉTHODOLOGIE

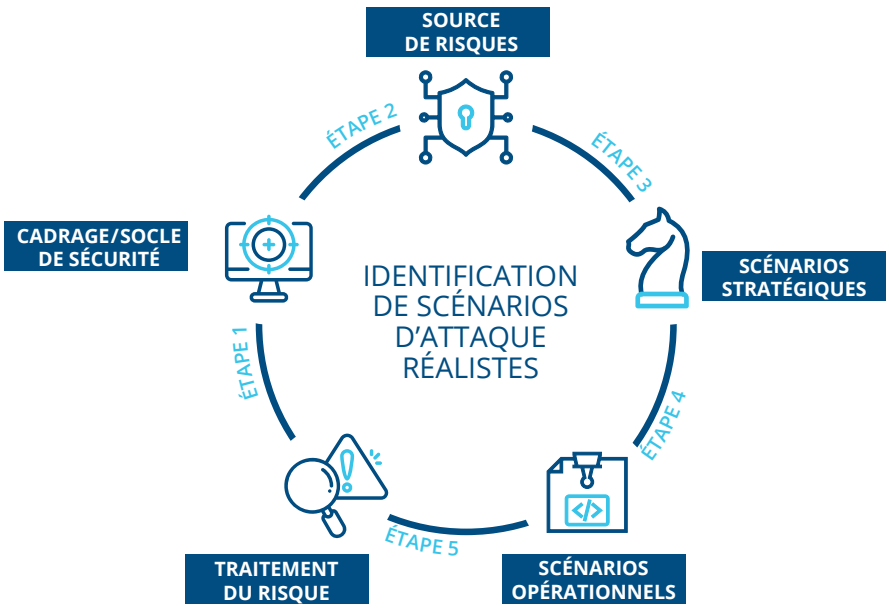
En France, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) a vu le jour en 1995 au sein de l'ancêtre de l'ANSSI. Cette méthode a été améliorée en profondeur en 2010 puis en 2018 avec EBIOS Risk Manager et bénéficie aujourd'hui de ses 20 ans d'expérience. Elle offre une approche pragmatique et opérationnelle dans le domaine de la gestion du risque cyber.

Nous avons donc fait le choix d'utiliser la méthode EBIOS Risk Manager pour mener cette analyse de risques.

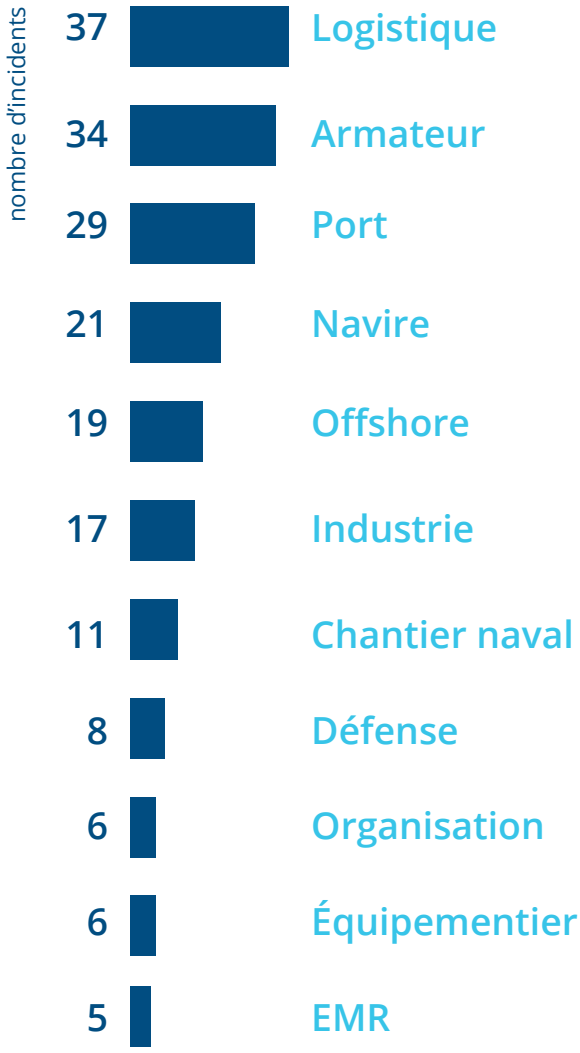
La méthode EBIOS Risk Manager adopte une approche de management du risque qui part du plus haut niveau (grandes missions de l'entreprise / organisme étudié, actifs à protéger) pour aboutir progressivement à l'identification de scénarios d'attaque réalistes et proposer un plan de traitement du risque adapté.



Pyramide du risque cyber - Méthode EBIOS Manager



SECTEURS D'ACTIVITÉ TOUCHÉS PAR DES INCIDENTS DE CYBERSÉCURITÉ MARITIME



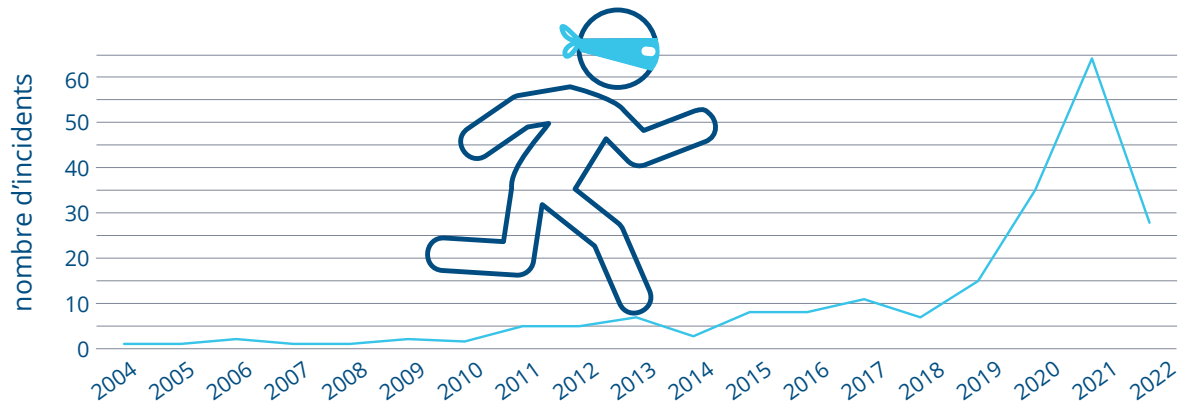
Le nombre d'évènements semble évoluer à la hausse, notamment au cours des dernières années. Cette hausse s'explique notamment par une augmentation de la surface d'attaque, de l'exposition de vulnérabilités, mais aussi de leur exploitation, notamment dans le cas d'attaques par rançongiciels.

ÉTAT DE LA MENACE

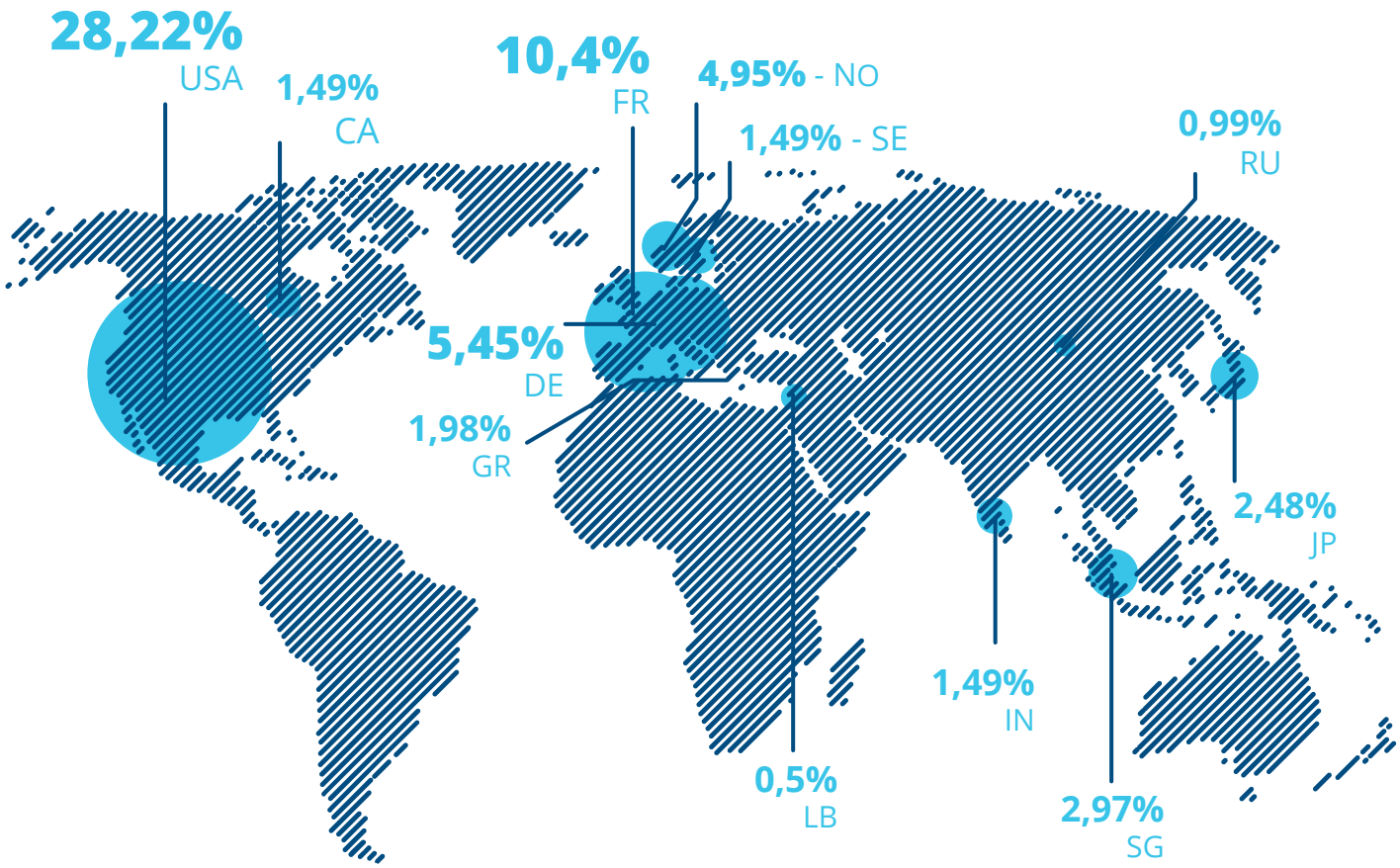
Les **codes malveillants/rançongiciels** sont les plus fréquents, devant les intrusions réseaux et les principaux pays sont les **États-Unis** et la **France.**

Le domaine de la **logistique** et de la **supply chain** est le plus touché devant les armateurs et les ports.

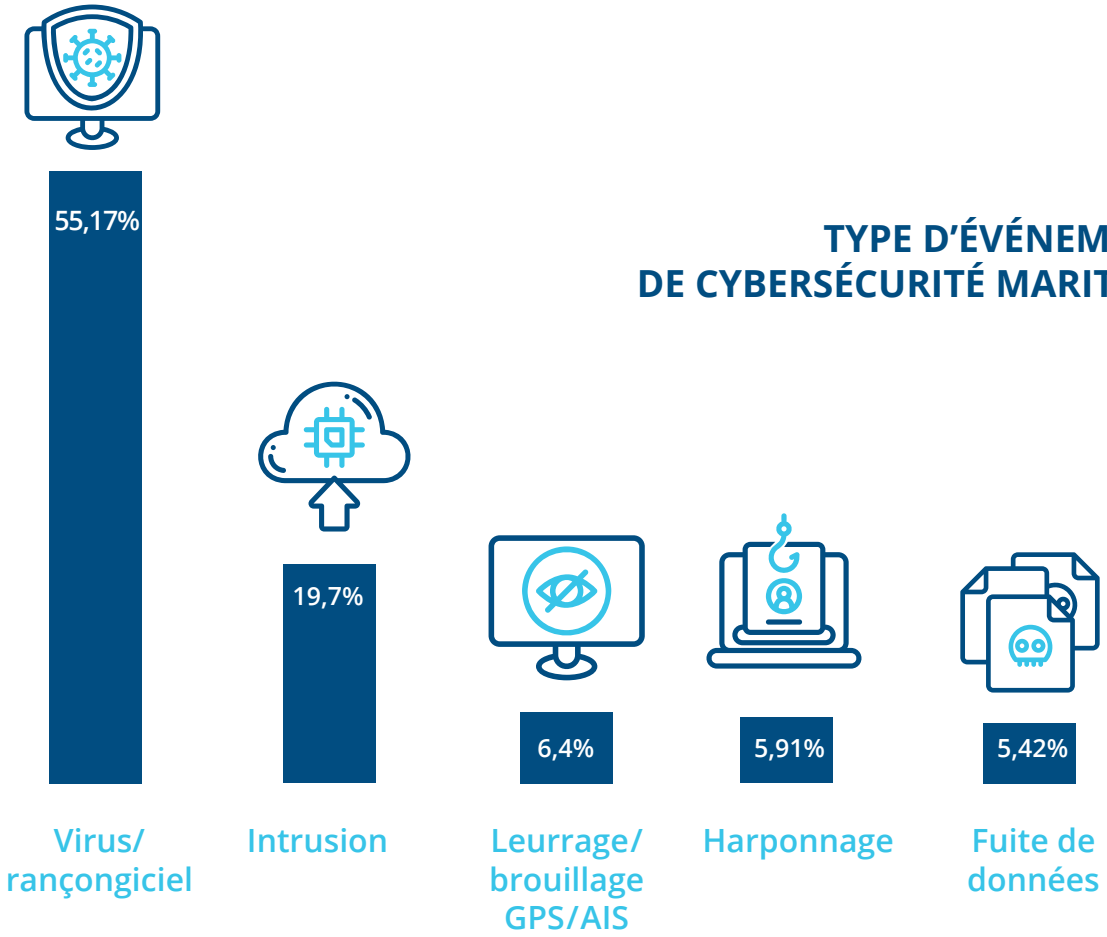
ÉVOLUTION DU NOMBRE D'INCIDENTS DE CYBERSÉCURITÉ MARITIME RENDUS PUBLICS



PAYS IMPACTÉS PAR DES INCIDENTS CYBER MARITIME



TYPE D'ÉVÉNEMENT DE CYBERSÉCURITÉ MARITIME



9 ÉVÉNEMENTS REDOUTÉS

Nous avons sélectionné les 9 événements redoutés des 2 niveaux de gravité les plus élevés : « critique » ou « catastrophique ».

À ces niveaux de gravité, la survenue de tels évènements serait caractérisée, d'une part, par une incapacité pour l'opérateur d'assurer son activité, avec des atteintes possiblement graves à la sécurité des biens, des personnes et de l'environnement. Et d'autre part, par un impact sur le secteur d'activité dans son ensemble, l'état et/ou les missions d'importance vitale.

Sans surprise, nous constatons que la grande majorité des événements redoutés jugés critiques concernent des atteintes à la disponibilité ou l'intégrité des processus et des actifs du domaine de l'Operational Technology (OT).

	ÉVÈNEMENTS REDOUTÉS	IMPACTS	GRAVITÉ
ER1	Atteinte à la disponibilité ou à l'intégrité des systèmes OT d'un navire essentiels à son contrôle et son opération (propulsion, gouverne, énergie, auxiliaire, stabilité/ballasts, hull-stress, contrôle des portes d'un RORO, Dynamic Positioning, etc.)	Perte de contrôle du navire dont les conséquences dépendent de la situation (a quai ou en mer), des conditions météo et de la zone de navigation (dangers) : incapacité à prendre la mer, incapacité à manœuvrer, naufrage (échouement, collision, chavirage, rupture de coque, ...)	Critique
ER14	Atteinte à la disponibilité ou à l'intégrité des systèmes OT essentiels au contrôle de tout une flotte de navires (propulsion, gouverne, énergie, auxiliaire, stabilité/ ballasts, hull-stress, etc.)	Perte de contrôle de tout ou partie des navires de la flotte dont les conséquences dépendent de la situation (a quai ou en mer), des conditions météo et de la zone de navigation (dangers) : incapacité à prendre la mer, incapacité à manœuvrer, naufrage (échouement, collision, chavirage, rupture de coque...)	Catastrophique
ER2	Atteinte à la disponibilité ou à l'intégrité des systèmes OT en passerelle utilisés pour la navigation, dont les équipements requis par le GMDSS (INS/IBS, ECDIS, GNSS, AIS, radar, sondeur, capteurs météo, loch, compas)	Perte des équipements de navigation électronique, dépend de la situation (à quai ou en mer), perturbation de la navigation (retards), erreur de navigation pouvant potentiellement mener à un naufrage selon les conditions météo, la zone de navigation (dangers).	Critique
ER3	Atteinte à l'intégrité des cartes électroniques utilisées pour la navigation (ENC) et diffusées par le SHOM et le PRIMAR vers l'ensemble de la flotte sous pavillon national	Erreur de navigation pouvant potentiellement mener à un naufrage selon les conditions météo et la zone de navigation (dangers). Impact potentiel sur l'ensemble de la flotte sous pavillon national. Tous les navires naviguant sur la zone concernée avec la carte compromise sont concernés.	Critique
ER21	Atteinte à la disponibilité ou l'intégrité des systèmes OT de contrôle des infrastructures portuaires maritimes (écluses, ponts, bassins, signalisation maritime...)	L'activité du port est fortement perturbée. Les navires ne peuvent plus entrer/sortir du port, possibles accidents physiques avec risques pour la vie humaine, le matériel, l'environnement.	Critique
ER10	Atteinte à la disponibilité ou l'intégrité des systèmes de surveillance du trafic (VTS) dans la Zone Maritime et Fluviale de Régulation du port (ZMFR)	L'activité du port est fortement perturbée. Les navires ne peuvent plus entrer ou sortir du port sauf éventuellement si météo favorable et de jour.	Critique
ER18	Atteinte à la disponibilité ou l'intégrité du Cargo Community System (CCS)	Paralysie du port : les marchandises ne peuvent plus entrer ou sortir du port. L'activité et la mission de la place portuaire est affectée dans son ensemble.	Critique
ER28	Atteinte à l'intégrité ou la disponibilité du système de gestion de l'énergie électrique du port (Transformateurs, Générateurs, Power Management Systems, UPS) provoquant un dysfonctionnement de l'alimentation électrique ou un blackout	Arrêt de l'approvisionnement en électricité. Toute l'infrastructure portuaire fonctionnant à l'électricité est à l'arrêt : Systèmes IT et OT, VTS, Feux, écluses, ponts, grues, entrepôts réfrigérés, alimentation des containers réfrigérés, alimentation des navires à quai, pompes, systèmes de sécurité et de sûreté (contrôle d'accès, portes automatiques). Possible destruction des équipements si variations du courant électrique en dehors de limites de fonctionnement (voltage, ampérage ou fréquence).	Critique
ER29	Atteinte à la disponibilité ou l'intégrité du Port Community System (PCS)	Impact sur la planification et l'organisation gestion des escales du ou des ports utilisateurs de la solution PCS. Une indisponibilité du PCS au-delà de 6h perturbe gravement la planification et l'organisation des escales des navires de l'ensemble des ports concernés	Critique

11 SCÉNARIOS D'ATTAQUE RETENUS

RECOMMANDATIONS

Des recommandations générales au secteur formulées dans le domaine de la gouvernance, de la protection, de la défense et de la résilience. À titre d'exemple :

- **la réglementation :**
  - réflexion sur le périmètre d'application de la LPM et de la directive NIS au secteur maritime ;
  - évolution du code ISPS et ISM de l'OMI pour mieux prendre en compte les risques cyber ;
- **l'intégration de la cyber sécurité dans la conception des systèmes (security by design) :**
  - définition de standards internationaux de cyber sécurité en particulier pour les navires ;
- **l'incitation à la classification cyber (BV NR659, DNV-GL RP 4096…) pour les nouveaux navires sous pavillon national ;**
- **la sensibilisation des acteurs et des employés du secteur ;**
- **la prise en compte de la cyber sécurité dans les relations de sous-traitance ;**
- **le renforcement du rôle du M-CERT : encourager l'adhésion, la notification des incidents et le partage d'informations cyber ;**
- **la réflexion sur l'opportunité de créer un SOC mutualisé pour les opérateurs du secteur.**

1 Attaque par Ransomware sur le SI d'un navire avec rebond vers les systèmes OT essentiels à la navigation.

2 Attaque par Ransomware sur le SI de l'ensemble des navires d'une flotte.

3 Sabotage des systèmes OT essentiels au contrôle du navire dans le but de perturber la navigation et/ou de provoquer un accident maritime (échouement, collision…).

4 Sabotage des systèmes OT d'une flotte de navires dans le but de paralyser l'activité de transport maritime d'un opérateur ou d'un pavillon.

5 Attaque par Ransomware sur le SI du port avec rebond vers les systèmes OT essentiels au contrôle de l'infrastructure portuaire (ponts, bassins, écluses…).

6 Attaque par Ransomware sur les systèmes de surveillance du trafic (VTS) essentiels au contrôle de la navigation dans la ZMR.

7 Sabotage des systèmes OT essentiels au contrôle de l'infrastructure portuaire (ponts, bassins, écluses) dans le but de perturber l'activité du port et/ou de détruire des équipements.

8 Sabotage du système d'alimentation électrique du port afin de paralyser les activités portuaires et/ou de détruire des équipements.

9 Sabotage des systèmes de surveillance du trafic (VTS) essentiels au contrôle de la navigation dans la ZMR dans le but de perturber l'activité du port.

10 Attaque par ransomware du ou des Port Community Systems (PCS) / Cargo Community Systems (CCS) hébergés par un fournisseur de service numérique portuaire.

11 Sabotage du ou des Port Community Systems (PCS) / Cargo Community Systems (CCS) hébergés par un fournisseur de service numérique portuaire afin de paralyser l'activité du ou des ports concernés.

Contact :

Didier Daoulas
Directeur du comité « Analyse des risques »
Ingénieur département Maritime - Bessé

didier.daoulas@sofimar.fr

L'étude détaillée est la propriété du SG Mer et comporte une mention de protection TLP Green, ce qui implique une diffusion limitée, restreinte au secteur maritime français.