Comité France Maritime

Centre de Coordination CYBER Du Monde Maritime

E-blueday Cybersécurité maritime

Attaques CYBER pendant la crise COVID-19

Le secteur maritime particulièrement touché

International Maritime Organization
79 323 abonnés
4 h · Modifié ·

A number of IMO's web-based services are currently unavailable, including IMO's public website. Service has been restored to the GISIS database, IMODOCS and Virtual Publications. The interruption of service was caused by a sophisticated cyber attack against the Organization's IT systems that overcame robust security measures in place. IMO IT technicians shut down key systems to prevent further damage from the attack. The IMO is working with UN IT and security experts to restore systems as soon as possible, identify the source of the attack, and further enhance security systems to prevent recurrence.

Voir la traduction

Suspecting Cyber Attack, MSC Reports Network Outage – Update

April 10, 2020 by Mike Schuler

Mars 2020 – Suisse (MSC)

Janvier 2020 – Elbe (Spoofing AIS)

EUROPEAN COAST GUARD FUNCTIONS FORUM

March 2020 UNCLASS – For Official Use Only

Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks (NY Times May 19)

Israel was behind a cyberattack that disrupted a major port in Iran, done in response to an attempt by the Revolutionary Guards to infiltrate an Israeli water facility.

Avril 2020 – Ormuz Pot de Bandar Abbas (Attaque ISR)

Sept 2020 – Int (CMA-CGM)

Mai 2020 – Californie (Spoofing AIS)

Sept 2020 – Int (GEFCO)

Med Europe Terminal

Actualités

/!\ ATTENTION CYBER ATTAQUE /!\

SUITE CYBER ATTAQUE VEUILLEZ NOTER LES ADRESSES DE SECOURS :

- RESPONSABLES D'EXPLOITATION : operations@intramar.fr
- EMPOTAGE / DEPOTAGE / COMMERCIAL / LITIGE : commercial@intramar.fr
- SHIPPLANNING : co@intramar.fr
- GARE / GATE : gare@intramar.fr
- FACTURATION : facturation@intramar.fr
- CONTENTIEUX contentieux@intramar.fr
- COMPTABILITE : compta@intramar.fr
- DAF : sarti.l@marseille-manutention.com
- SERVICE IT : it@intramar.fr
- MAINTENANCE / TECHNIQUE : dt@intramar.fr

Voir toutes les actualités

Mars 2020 – Marseille / FOS - Attaque Région SUD

2020 – Mediterranée (Brouillage GPS)

Jan 2020 – Mer de Chine (Spoofing AIS)

Incidents 2017 – 2020 – Impacts / analyse

Entité attaquée	Date	Impact	Analyse
MAERSK	2017	49 000 PC et 1200 applications inopérantes. Perte du partage de fichiers et des messageries	Le **regroupement des activités sur une même structure** ont fragilisé considérablement le groupe
COSCO US	2018	Perte d'accès à Internet et impact sur le fonctionnement des messageries et téléphones	Un **PCA / PRA robuste** mis en place a permis de réduire l'impact de l'attaque
Ports de San Diego / Barcelone	2018	Pertes de systèmes divers (dédouanement, gestion des stationnements)	L'attaque à une semaine d'intervalle aurait pu être évitée avec une **meilleure coordination**
Port de Bandar Abbas	2020	Incapacité de mettre en œuvre les terminaux de chargement et de déchargement	Un port « non critique » dans une **attaque préventive,** ciblé par un pays entrainant une riposte immédiate
MSC	2020	Services inopérants pendant plus de 12h Page web inaccessible pendant plusieurs jours	Les **services hébergés localement** ont permis de continuer à l'opérateur de fonctionner sur certaines régions
MED EUROPE TERMINAL	2020	Services Internet bloqués ayant impacté le portail web et les messageries.	L'opérateur maritime a été **victime collatérale** d'une attaque subie par la région Sud pendant le confinement
Systèmes GNSS/AIS	2018 - 2020	Saturation de récepteurs AIS (observés en Méditerranée en 2019, en Chine aux USA en 2020) Brouillages permanent GPS observés en Méditerranée Orientale, en Mer de Chine et en Mer Noire	Le brouillage ou le Spoofing (saturation) des moyens GNSS et/ou AIS représente un réel danger pour la navigation. Observables dans leurs formes les plus grossières (de l'heure uniquement) les attaques sur les systèmes GNSS/AIS peuvent à terme fausser l'ensemble des données maritimes.
CARNIVAL	2020	Perte de données clients et employés. Perte d'activité sur la croisière (réservations)	Attaque classique par **ransomware** ayant chiffré une partie des systèmes IT et des données.
DNV-GL	2020	Espionnage au profit d'un état - Vol de données Image de la société écornée	Les sociétés de classe sont particulièrement **exposées à ce type d'attaque**

Stratégie

La cybersécurité concerne tout le monde, mais rares sont encore ceux qui se sentent impliqués

Une dispersion des initiatives nuit à l'efficacité

L'urgente nécessité:
- De s'organiser
- De résister
- De partager
- De protéger les plus fragiles

La Cybersécurité est une fonction induite en soutien du secteur maritime mais reste à ce jour trop souvent une variable d'ajustement

Une trop faible présence française dans les projets Européens

Le besoin d'implication des administrations exprimé par le secteur entier.

Faire face au besoin du secteur maritime

L'urgente nécessité:
- De s'organiser
- D'interopérer
- De partager
- De protéger les plus fragiles

Une optimisation des ressources

Donner une impulsion pour Inscrire la cybersécurité sur le long terme dans un secteur concurentiel

Une capacité à répondre aux initiatives européennes

Le besoin d'un service public

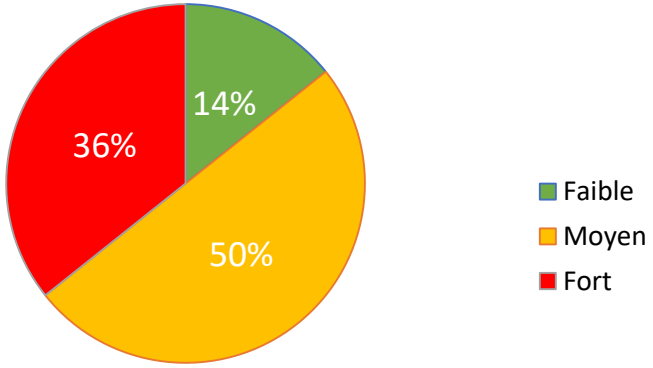
PREMIER MINISTRE
Liberté
Égalité
Fraternité

Les benefice d'un centre de coordination

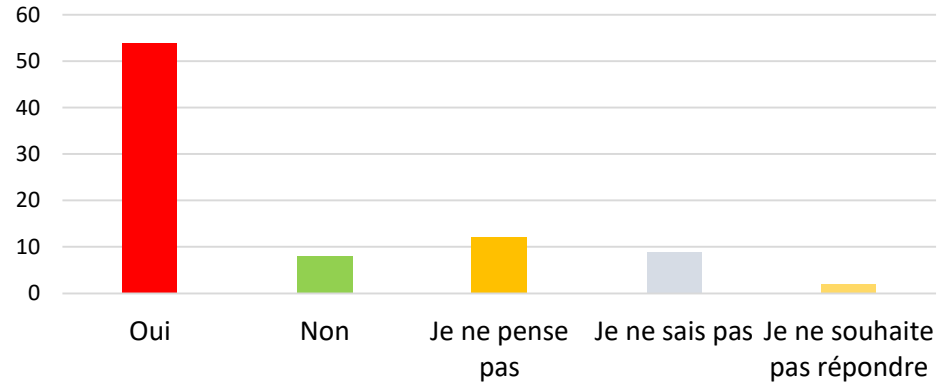
QUESTIONNAIRE CYBER 2020

Exposition de la filière - donnéee 2020 sur un echelon de 171 organismes ayant répondus

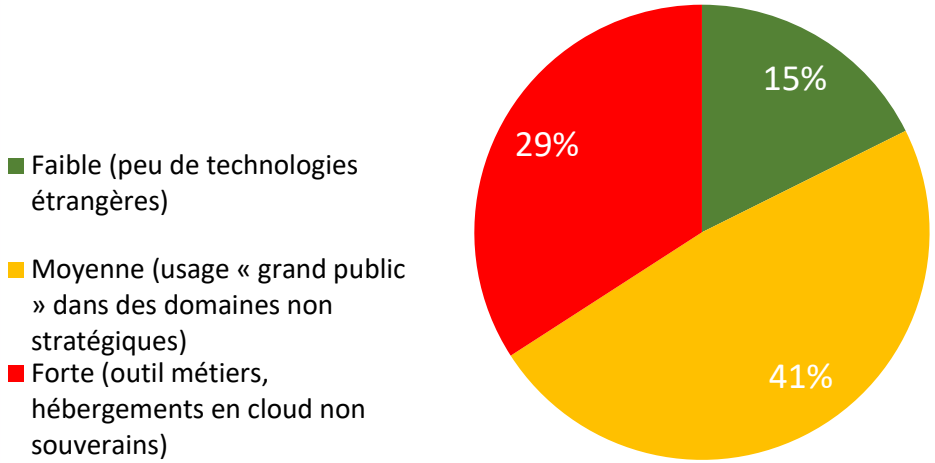
Niveau d'exposition Estimé face à la menace Cyber



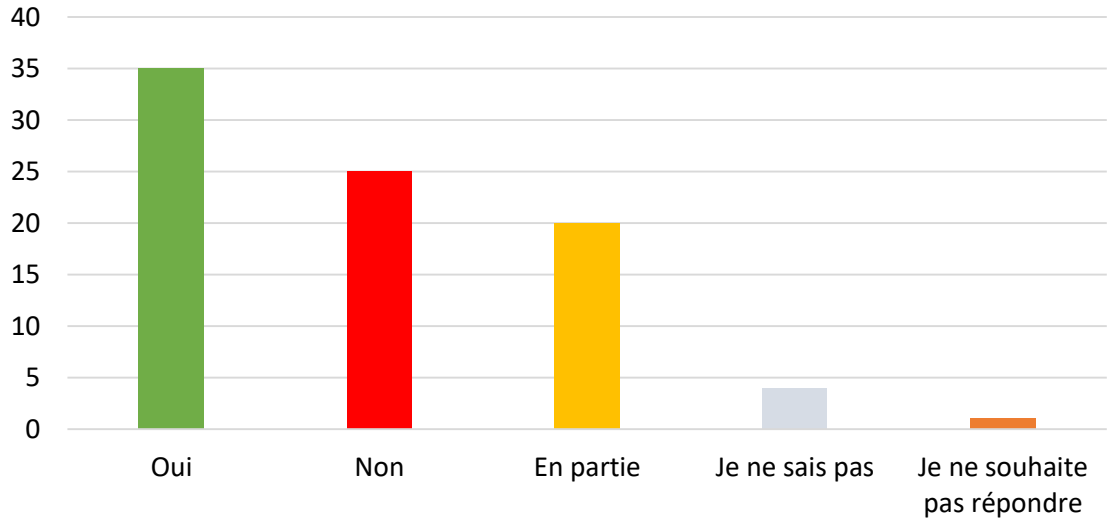
Tentative d'attaque cyber contre l'entité



Dépendance aux technologies étrangères



Services chargés de cybersécurité au sein de l'entité

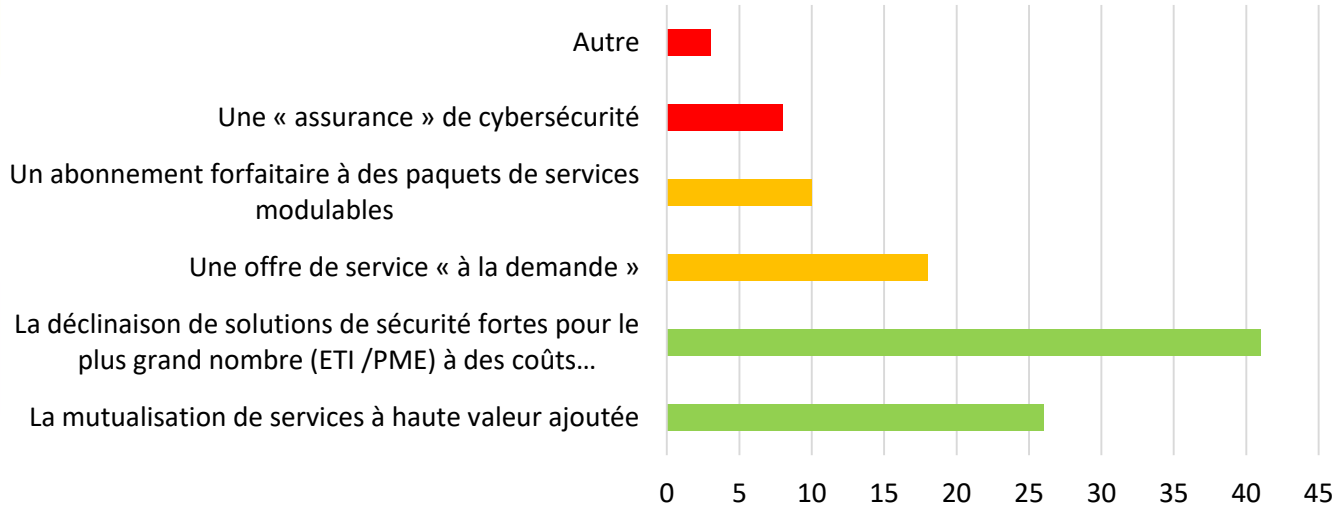


PREMIER MINISTRE
Liberté
Égalité
Fraternité

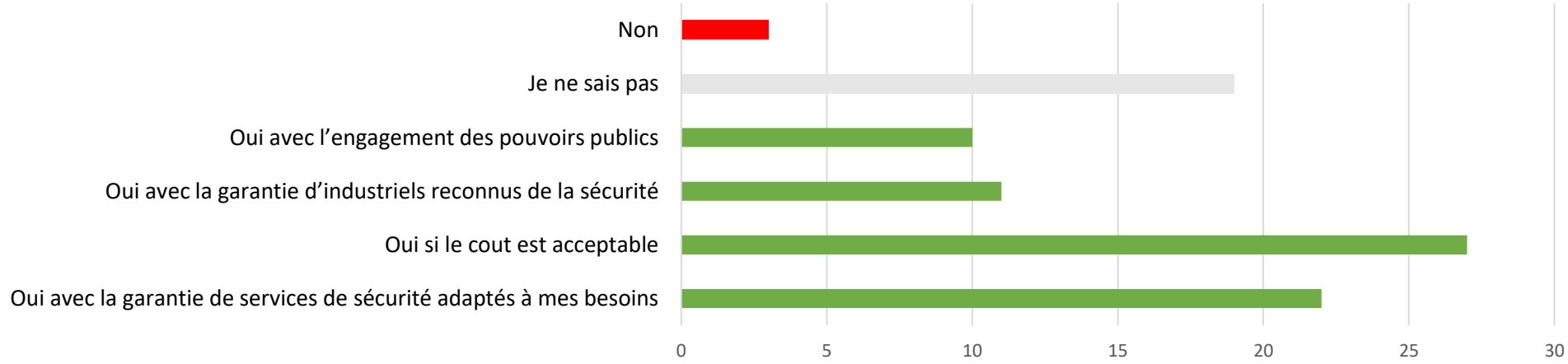
La perception du future centre de coordination Cyber

Effets recherchés

Les facteurs d'efficacité d'un centre de cybersécurité



Participation au centre de cybersécurité



PREMIER MINISTRE

Liberté
Égalité
Fraternité

La Cybersécurité du Monde Maritime

Conseil Cyber du Monde Maritime (C2M2)

COMEX | C. Analyse des risques | C. Prospective et régulation

Centre de coordination

Association de préfiguration puis GIP

Comité stratégique de pilotage | Conseil d'administration

M-ISAC

Analyser le risque et partager les informations CYBER

M-SOC	M – CERT	EXP / FORM
Surveiller les activités	Détecter les attaques et incidents et les traiter efficacement	Investiguer et collecter les éléments de preuves
	Gérer les situations de crise en cas d'incidents majeurs	Améliorer la cybersécurité des systèmes

Administrations

Opérateurs portuaires

Ports

PME / ETI maritime & offshore

Opérateurs maritime

PREMIER MINISTRE

Liberté Égalité Fraternité