GOUVERNEMENT

Liberté
Égalité
Fraternité

Ports « cybersécurisés »

Guide de bonnes pratiques pour la cybersécurité dans le secteur portuaire

Juin 2021

INFORMATIONS GÉNÉRALES

Version :	**V1 du 04 juin 2021**.
Supervision :	**Nicolas TRIFT**, Sous-directeur des ports et du transport fluvial (DGITM/DST/PTF)
Relecture :	**Stéphanie CUBIER**, Adjointe au Sous-directeur des ports et du transport fluvial (DGITM/DST/PTF)
Coordination :	**Cédric LOESCHER**, Chef du bureau de la sûreté portuaire et fluviale (DGITM/DST/PTF/PTF5)
Rédaction :	**Erwan DELAN**, Auditeur national de sûreté portuaire, référent cybersécurité portuaire (DGITM/DST/PTF/PTF5)
Illustration :	**Renan KREMER**, Chargé de mission « intelligence économique portuaire » (DGITM/DST/PTF/PTF4)
Contributions :	**Bruno BENDER**, Coordinateur cyber pour le domaine maritime (Secrétariat Général de la Mer)
	Sylvie ANDRAUD, Coordinateur sectoriel (SGDSN/ANSSI)
	Laurent BANITZ, Chef de la mission cybersécurité et sûreté des navires (DGITM/DAM/STEN)
	Franck VAYNE, Commandant en second de la section de recherches de la Gendarmerie maritime
	Mathilde POLLET, Responsable des Affaires Economiques et Européennes de l'Union des Ports de France
	Jérôme BESANCENOT, Chef du Service Développement des Systèmes d'Information de HAROPA – Port du HAVRE
	Gildas REUL, Agent de sûreté portuaire du Grand Port Maritime du HAVRE
	Paul FRANQUART, AQSSI du Grand Port Maritime de MARSEILLE
	Benoît DESCHAMPS, Chef du Service Systèmes d'Informations du Grand Port Maritime de la Martinique
	Laurence MATRINGE, Secrétaire Générale de Ports de PARIS – HAROPA, précédemment Adjointe au Sous-directeur des ports et du transport fluvial
	Jean-Luc ZVUNKA, Responsable du pôle sûreté, sécurité et affaires régaliennes chez Ports Rade de TOULON
	Clarisse CERTENAIS, Chargée de sûreté et sécurité portuaire à la Direction des Ports de la Région Bretagne
	Catherine GABAY, Directrice Adjointe du Contrôle du Spectre à l'Agence Nationale des Fréquences (ANFR)
	Jean-Louis SCHMITZ, Référent maritime à l'Agence Nationale des Fréquences (ANFR)
	Damien BELLIER, Coordonnateur interministériel délégué GALILEO
	Stéphanie BAILLY, Chargée de mission « services portuaires et concurrence » (DGITM/DST/PTF/PTF2)
	Gabriel ARONICA, Chef de projet transition écologique et numérique des ports (DGITM/DST/PTF/PTF4)

SIGLES

AIS	Système d'identification automatique (en anglais, « Automatic Identification System »)
API	Interface de programmation d'application (en anglais, « Application Programming Interface »)
ASC	Agent de sûreté de la compagnie
ASIP	Agent de sûreté de l'installation portuaire
ASN	Agent de sûreté du navire
ASP	Agent de sûreté portuaire
BMI	Bureau maritime international (en anglais, « International Maritime Bureau » - IMB)
CCS	*Cargo Community System* (Système informatique d'échanges d'informations liées aux flux physiques de marchandises)
CE	Commission européenne
DSI	Directeur de la sécurité de l'information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EM	Etat membre
EMSWe	Système de guichet unique maritime européen (en anglais, « European Maritime Single Window environment »)
ERP	Progiciel de gestion intégré – PGI (en anglais, « Enterprise Resource Planning »)
ESIP	Evaluation de sûreté de l'installation portuaire
ESP	Evaluation de sûreté portuaire
GPM	Grand port maritime
GNSS/GPS	Géolocalisation et Navigation par Système Satellite / Système de positionnement global (en anglais, « Global Positioning System »
GUMP	Guichet unique maritime et portuaire
ICS	Système de contrôle industriel (en anglais, « Industrial Control System »)
IEC	Commission électrotechnique internationale (en anglais, « International Electrotechnical Commission »)
IoT	Internet des Objets – IdO (en anglais, « Internet of Things »)
ISM (code)	Code international de gestion de la sécurité (en anglais, « International Safety Management »)
ISO	Organisation internationale de normalisation (en anglais, « International Organization for Standardization »)
ISPS (code)	Code international pour la sécurité des navires et des installations portuaire (en anglais, « International Ship and Port Facility Security Code »)
IT	Technologie de l'information
LAN	Réseau informatique local (en anglais, « Local Area Network »)
NIST	Institut national des normes et de la technologie (en anglais, « National Institute of Standards and Technology »)
OMI	Organisation maritime internationale (en anglais, « International Maritime Organization » - OMI)
OIV	Opérateur d'importance vitale
OSE	Opérateur de services essentiels
OT	Technologie d'exploitation (en anglais, « Operational Technology »)
PCS	Système communautaire portuaire (en anglais, « Port Community System »)
PSIP	Plan de sûreté de l'installation portuaire
PSP	Plan de sûreté portuaire
PSSI	Politique de sécurité du système d'information
RGPD	Règlement general sur la protection des données
RSSI	Responsable de la sécurité des systèmes d'information (en anglais, CISO - « Chief information security officer »)
RTG	Responsable de la transformation digitale (en anglais, CDO – « Chief Digital Officer »)
SI	Système industriel (équivalent « OT »)
SIE	Système d'Information d'Entreprise
SII	Système d'Information Industriel
SIIV	Système d'information d'importance vitale
SOC	Centre d'opérations de cybersécurité
TI	Technologie de l'Information (en anglais, IT - « Information Technology »)
TIC	Technologies de l'information et de la communication
TOS	Système d'exploitation de terminaux (en anglais, « Terminal Operating System»)
UE	Union européenne
USB	Bus série universel (en anglais, « Universal Serial Bus»)
VHF	Très haute fréquence (en anglais, « Very High Frequency »)
VLAN	LAN virtuel (en anglais, « Virtual Local Area Network »)
VPN	Réseau privé virtuel (en anglais, « Virtual Private Network »)
VTMIS	Système d'Information de Gestion du Trafic des Navires (en anglais, « Vessel Traffic Management Information System »)
VTS	Suivi du trafic maritime (en anglais « Vessel Traffic Service »)

TABLE DES MATIÈRES

PRÉAMBULE

Le transport maritime est une activité essentielle pour l'économie de la France. Il repose notamment sur 50 ports maritimes et quelque 250 installations portuaires, soumis au code ISPS, d'une grande diversité en termes d'étendue, d'activités, d'organisation, d'acteurs et d'enjeux de développement.

La tendance mondiale à la numérisation et les politiques et réglementations récentes obligent les ports maritimes à relever de nouveaux défis en matière de technologies de l'information et de la communication. Ils s'appuient en effet de plus en plus sur les technologies pour gagner en compétitivité, se conformer à certaines normes et politiques publiques et améliorer leur fonctionnement.

Ces évolutions génèrent de nouveaux enjeux et défis dans le domaine de la cybersécurité, à la fois dans les domaines des technologies de l'information (TI) et des systèmes industriels (SI).

Conscient des cybermenaces qui pèsent sur les ports et le transport maritime, le ministère de la mer et le ministère chargé des transports en lien avec le Secrétariat général de la mer (SG Mer) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI), ont pleinement intégré la cybersécurité comme une orientation stratégique majeure de la stratégie nationale portuaire validée par le Premier ministre lors du Comité interministériel de la mer du 22 janvier 2021.

Dans cette perspective, le présent guide, constitue la déclinaison française du guide de l'Agence européenne chargée de la sécurité des réseaux et de l'information « ENISA » intitulé Port Cybersecurity – Good practices for cybersecurity in the maritime sector. Il vise à proposer des recommandations et bonnes pratiques utiles à tous les acteurs des ports maritimes dans leur diversité pour que ceux qui le souhaitent, selon leurs capacités (organisationnelles, techniques, humaines, financières), puissent adapter leur action en matière de cybersécurité.

Il a pour ambition d'accompagner l'intégration ainsi des ports maritimes français au cadre européen de coopération en matière de cybersécurité.

Nicolas TRIFT, Sous-directeur des ports et du transport fluvial

INTRODUCTION

L'Union européenne a identifié les ports maritimes comme des infrastructures essentielles et les a définis comme « toute zone spécifiée de terre et d'eau, avec des limites définies par l'État membre dans lequel le port est situé, comportant des infrastructures et des équipements destinés à faciliter les opérations de transport maritime commercial » aux termes de la Directive 2005/65/CE du 26 octobre 2005 relative à l'amélioration de la sûreté des ports.

Les ports maritimes jouent un rôle majeur à différents niveaux dans de nombreux secteurs et sont pleinement interconnectés aux autres modes de transport (fluvial, ferroviaire, routier). En tant que principal vecteur d'importations et d'exportations (produits alimentaires, matières premières, etc.) avec le reste du Monde, ils constituent également des nœuds importants pour le transport de passagers et de véhicules inter et extra Union européenne.

Depuis plusieurs années, ils intègrent les transformations numériques afin de relever les défis émergents (digitalisation des flux logistiques, nouveaux services digitaux, etc.), d'optimiser les processus existants et d'introduire de nouvelles capacités, telles que la surveillance en temps réel des opérations. Cette numérisation s'est concentrée sur l'interconnectivité des actifs des technologies de l'information (TI) et des systèmes industriels (SI) et sur l'introduction de nouveaux catalyseurs technologiques, tels que le cloud computing, les megadonnées ou encore l'Internet des objets (IoT).

Cette transformation numérique augmente l'exposition des acteurs portuaires aux cybermenaces et a également entraîné une modification du profil de cyber-risque du secteur, comme en témoigne la prolifération des incidents de cybersécurité dans les ports au cours des dernières années, tels la cyberattaque du port d'ANVERS (2011), le sabotage NotPetya et son impact sur MAERSK (2017), la vague d'attaques de rançongiciels contre les ports de BARCELONE et SAN DIEGO ou encore récemment contre CMA-CGM (2020).

En résultent des impacts importants en termes financier, de sécurité, d'image, etc. pour les acteurs portuaires, publics comme privés.

A l'heure où nos ports maritimes deviennent des « ports intelligents », associant infrastructures et services performants, de surcroît dans un contexte marqué, à titre structurel, par les enjeux de transition écologique et, à titre conjoncturel (souhaitons-le), par une crise sanitaire qui favorise le développement des cyberattaques, les défis de cybersécurité qui doivent être relevés sont majeurs pour que les ports du futur exploitent pleinement le potentiel des nouvelles technologies en toute « cyber-sécurité ».

Contexte

Le présent guide s'inscrit dans un contexte d'accroissement et de multiplication des cybermenaces à mesure que les acteurs maritimes opèrent leur transition numérique.

La stratégie européenne de sécurité maritime (SESM, en anglais « EUMSS »), adoptée en 2014 et révisée en 2018, a ainsi identifié les cybermenaces parmi les risques et menaces pour la sécurité maritime au même titre que les autres actes illicites intentionnels en mer et dans les ports contre les navires, les cargaisons, les équipages et les passagers, les ports et les installations portuaires et les infrastructures maritimes et énergétiques critiques.

Prenant conscience de ces enjeux, le comité interministériel de la mer (CIMer) de novembre 2018 a ainsi prévu la création en France d'une structure de gouvernance dédiée au risque cyber dans le secteur maritime.

Le premier Conseil de Cybersécurité du Monde Maritime (C2M2) s'est ainsi tenu le 7 novembre 2019, sous la présidence du Secrétaire Général de la Mer (SGMer). Avec l'appui de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), il est destiné à coordonner des acteurs privés et publics, afin d'assurer une meilleure connaissance des cybermenaces et de renforcer la capacité d'action collective du secteur maritime.

En parallèle, le comité interministériel de la mer (CIMer) du 22 janvier 2021 a validé la stratégie nationale portuaire - axée notamment sur la transition écologique et numérique des ports maritimes - dont le principe avait été acté lors du CIMer de novembre 2019.

Afin d'allier cybersécurité et innovation, celle-ci préconise notamment la création d'une communauté de responsables de la transformation digitale (« chief digital officers »), chargés d'animer la transformation numérique des grands ports maritimes sur ces deux volets. Cette communauté devra partager les expérimentations, initiatives et bonnes pratiques de certains grands ports maritimes dans le domaine de la cybersécurité pour permettre leur diffusion à l'ensemble des ports maritimes.

Focus sur l'objectif stratégique n°15
de la stratégie nationale portuaire 2020-2025
« Assurer la résilience numérique des ports »

Le présent objectif vise à ce que les ports développent de nouveaux services à partir des technologies digitales émergentes en les intégrant dans leurs feuilles de route digitales, à l'instar du Réseau 5G, de l'Internet des objets (IoT), de la *blockchain* ou de l'intelligence artificielle, du *Big Data* ou de l'interopérabilité des systèmes d'information portuaires (PCS) et logistiques (CCS).

La digitalisation est désormais un élément compétitif primordial pour les ports maritimes. Au fur et à mesure que la digitalisation des opérations se développe, des nouveaux enjeux et défis s'imposent dans le domaine de la cybersécurité. Au-delà des navires, les interconnexions des systèmes d'information traitant de la gestion des escales, du fret, l'inspection passagers, les systèmes de gestion technique ou de télécommunication, la supervision du trafic ou encore le contrôle des ouvrages (ponts, écluses, bassins…) sont potentiellement corruptibles.

Face à ces risques, il devient indispensable de partager les expérimentations et les initiatives des grands ports maritimes dans le domaine de la cybersécurité, s'appuyer sur une initiative pilotée pour structurer et fédérer les efforts des places portuaires dans ce domaine et diffuser des recommandations utiles à tous les ports dans leur diversité, pour que tous puissent, chacun à son niveau, adapter leur action en matière de cybersécurité et de développer et mutualiser des solutions de cybersécurité.

Dans ce cadre, l'Etat développe un guide de bonnes pratiques pour la cybersécurité dans le secteur portuaire en ligne avec les directives du guide ENISA, en plaçant les ports français dans un cadre européen de coopération.

Action 20 : développer un guide de bonnes pratiques dans le domaine de la cybersécurité portuaire en ligne avec les directives ENISA**. Pilote :** DGITM**. Echéance :** 2021.

Action 21 : favoriser le développement de solutions de cybersécurité (cf. sécurisation des PCS/CCS, des réseaux électriques, etc.) dans le cadre du Plan de relance et de la stratégie d'accélération cybersécurité pilotée par la Direction générale des entreprises (DGE). **Pilote :** CFM (C2M2)/DGE. **Echéance : 2021.**

Action 22 : développer les outils numériques au service de la performance portuaire, de la sécurisation des chaînes logistiques et de l'innovation. Les compétences et les expériences des responsables de la transformation digitale (« chief digital officers ») des ports seront mutualisées, au sein de la communauté mise en place, afin d'accélérer les mutations et de préparer le port du futur**. Pilote :** GPM**. Echéance :** 2021**.**

Le présent guide constitue ainsi un premier outil mis à la disposition des acteurs portuaires, pendant, pour le secteur portuaire, des guides élaborés conjointement par la Direction des Affaires Maritimes et l'ANSSI en 2017 et 2019 à destination des compagnies maritime. Il se présente clairement comme une déclinaison française du guide de l'Agence européenne chargée de la sécurité des réseaux et de l'information « ENISA » intitulé Port Cybersecurity – Good practices for cybersecurity in the maritime sector, publié en novembre 2019.

Objectifs

Le présent guide a comme principaux objectifs de permettre :

- d'identifier les actifs portuaires à cybersécuriser et ce de manière suffisamment générique pour que tous les ports dans leur diversité puissent s'impliquer dans une démarche de cybersécurisation active ;

- de cartographier les cybermenaces, les enjeux de cybersécurité pertinents pesant sur ces actifs portuaires et mettre en évidence certains scénarios de cyberattaques pour analyser le niveau de maîtrise des risques numériques ;

- de diffuser un socle commun de bonnes pratiques à adopter au sein de l'écosystème portuaire, tant en ce qui concerne les systèmes informatiques « IT » que les systèmes industriels « OT », pour assurer la cybersécurité des systèmes et services portuaires ;

pour, in fine, constituer une boîte à outils permettant aux acteurs portuaires mentionnés ci-après de réaliser un auto-diagnostic « cyber ».

Il se veut par ailleurs comme un outil de référence pour promouvoir la collaboration au sein de l'écosystème des ports maritimes en France et sensibiliser aux cybermenaces pertinentes.

Publics

Le présent guide s'adresse à tous les acteurs de l'écosystème portuaire impliqués dans les opérations portuaires et qui, pour la plupart, font également partie de la chaîne logistique, à savoir : les instances dirigeantes du port (autorités portuaires), les exploitants d'installations portuaires, les opérateurs portuaires, les sociétés de transport (compagnies maritimes, compagnies ferroviaires, etc.), tous les prestataires de services indispensables aux opérations portuaires (pilotes, manutentionnaires, etc.), mais aussi les représentants des services locaux de l'Etat - notamment les membres des comités de locaux de sûreté portuaire et groupes d'experts en sûreté portuaire pilotés par les préfectures - (police, gendarmerie, douanes, etc.).

Il s'adresse in fine plus particulièrement aux personnes en charge de la sécurité informatique au sein de cet écosystème portuaire ou concernées au quotidien par la prévention des actes illicites intentionnels contre le transport maritime et les opérations portuaires (RSSI, DSI, ASP, ASIP, ASC, ASN, etc.).

Il peut également être utile à d'autres acteurs de l'écosystème portuaire : les associations locales portuaires - notamment celles dont les membres sont en charge des questions de sécurité informatique, les responsables informatiques des entreprises en interaction avec les ports - notamment les sociétés de logistique, etc.

Méthode

Le présent guide a été élaboré selon la méthode suivante :

1° Constitution d'un groupe de travail représentatif des acteurs portuaires à l'initiative de la Sous-direction des ports et du transport fluvial (PTF) du ministère chargé des transports, en liaison avec le Secrétariat Général de la Mer (SG Mer) et l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

Constitué le 13 décembre 2019, le groupe de travail a tenu sa première réunion le 7 janvier 2020 qui a permis d'identifier les actions en cours et les guides existants, avec le choix de se positionner dans un cadre européen pour faciliter les échanges et les partenariats.

2° « Traduction » de l'étude de l'ENISA « Port cybsersecurity – Good practices for cybersecurity in the maritime sector » de novembre 2019 qui est apparue aux membres du groupe de travail comme constituant un outil totalement pertinent, méritant simplement d'être traduite et adaptée aux enjeux nationaux.

3° Elaboration d'un questionnaire « Cartographie en matière de cybersécurité des ports et installations portuaires » diffusé le 25 mai 2020 aux agents de sûreté des ports (ASP) et agents de sûreté des installations portuaires (ASIP) de métropole et d'outre-mer ainsi qu'aux capitaineries et aux centres régionaux opérationnels de surveillance et de sauvetage (CROSS), avec lien « Limesurvey » actif jusqu'au 19 juin 2020 (voir focus ci-après).

4° Enrichissement de la « traduction » du guide à partir des travaux du groupe de travail et des retours aux questionnaires au cours de l'été 2020.

5° Diffusion d'une V0 « bêta » du guide aux acteurs portuaires volontaires pour le tester sur le terrain (hiver 2020-2021).

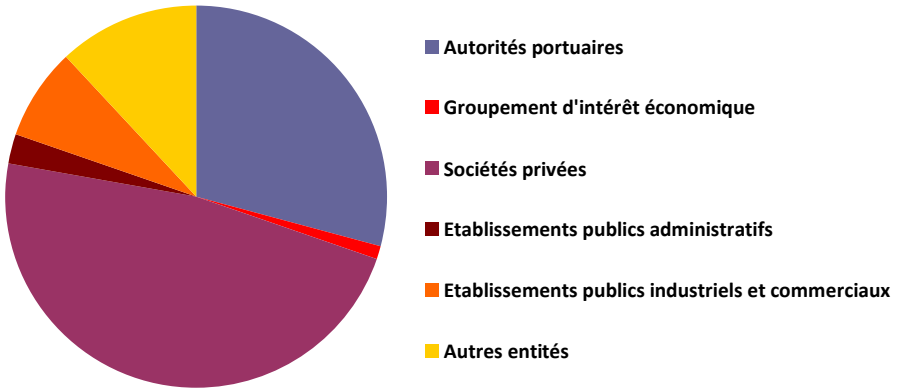
6° Finalisation de la version V1 du guide et diffusion aux acteurs des places portuaires (printemps 2021).

Focus sur le questionnaire « Cartographie en matière de cybersécurité des ports et installations portuaires »

143 entités (sur un total potentiel de 293 entités) ont répondu à ce questionnaire. Parmi elles, 50 se sont uniquement identifiées sans répondre aux différentes questions. Les statistiques et l'analyse sont donc basées sur les réponses fournies par les 93 entités ayant répondu à l'ensemble des questions.

La répartition est la suivante :

- 22 autorités portuaires soit 23,7% ;
- 1 groupement d'intérêt économique (GIE) soit 1% ;
- 36 sociétés privées soit 38,7% ;
- 2 établissements publics administratifs (EPA) soit 2% ;
- 6 établissements publics industriel et commercial (EPIC) soit 6.4%
- 9 entités autre soit 9,7%.



Majoritairement ces entités sont constituées par moins de 250 employés.

Pour ces entités, le risque cyber est considéré comme « moyen » dans 55,8 % des cas et 70 % des entités estiment avoir été la cible d'une cyber-attaque.

87 % d'entre elles accordent à la cybersécurité une priorité moyenne ou forte dans le développement de leur activité.

Afin de remédier aux failles en matière de cybersécurité, les entités ont essentiellement mis l'accent sur les volets « formation / sensibilisation de leur personnel » (environ 41%), « sécurisation des systèmes de communication » (appareils interconnectés ou postes de travail mutualisés) (environ 21 %).

Dans la quasi-totalité des cas, la gestion des cyber-risques est traitée en interne à l'entreprise, parfois même basé à l'étranger (stratégie de groupe).

Malgré, l'importance portée à la cybersécurité, dans le cas où l'entité dispose d'un plan de continuité d'activité, la cybersécurité est très peu prise en compte (environ 50 %). Alors que 82 % des entités disposent d'une politique dans le domaine.

73 % des agents de sûreté portuaire (ASP) ou agents de sûreté de l'installation portuaire (ASIP) travaillent avec les responsables cybersécurité.

1. APPREHENDER LE PAYSAGE PORTUAIRE FRANÇAIS

1.1 Cadre réglementaire

La cybersécurité des ports s'inscrit dans un cadre réglementaire international, européen et national qui reste récent et met en lumière les trois dimensions contemporaines des ports qui regroupement à la fois des infrastructures, des services et des données.

1.1.1 Cadre réglementaire de la « sûreté des infrastructures portuaires »

Le Code ISPS - Code international pour la sécurité des navires et des installations portuaires (International Ship and Port Facility Security Code), ajouté à la Convention sur la sauvegarde de la vie humaine en mer (SOLAS) en décembre 2002, reconnaît le rôle des installations portuaires dans la sûreté portuaire et maritime et définit les exigences et recommandations que les installations portuaires doivent suivre.

Il a été défini pour traiter la sûreté des ports, mais les exigences peuvent également être liées à la cybersécurité des ports dans une certaine mesure (exigences de contrôle d'accès et d'authentification).

Il oblige à établir une évaluation de sûreté des ports et installations portuaires pour identifier les principaux points vulnérables, les menaces et contre-mesures possibles et un plan de sûreté pour identifier, pour chacun des différents niveaux de sûreté, les procédures à suivre, les mesures à mettre en place et les actions à entreprendre.

L'évaluation de sûreté doit notamment aborder, dans le cas d'une installation portuaire, les aspects suivants : sécurité physique, intégrité structurelle, systèmes de protection du personnel, procédures, systèmes de radio et de télécommunication, y compris les systèmes et réseaux informatiques et les infrastructures de transport pertinentes.

Le plan de sûreté doit aborder l'accès à l'installation portuaire, les zones réglementées au sein de l'installation portuaire, la manutention de la cargaison, la livraison des provisions de bord et le contrôle de la sécurité de l'installation portuaire.

Le Code ISPS a été repris au niveau européen par le règlement (CE) 725/2004 du 31 mars 2004 qui se concentre sur l'amélioration de la sûreté des navires et des installations portuaires et par la directive 2005/65/CE du 26 octobre 2005 qui s'attache à l'amélioration de la sûreté des ports.

Est ainsi repris le principe de l'établissement par les Etats membres d'évaluations de sûreté des ports et des installations portuaires et, par les autorités portuaires et les exploitants d'installations portuaires, de plans de sûreté dont la mise en œuvre est contrôlée par les Etats membres.

1.1.2 Cadre réglementaire de la « sécurité des services portuaires »

Deux types de réglementations s'appliquent à la sécurité des services portuaires, selon qu'ils relèvent d'opérateurs d'importance vitale (OIV) ou d'opérateurs de services essentiels (OSE).

1.1.2.1 Cadre réglementaire applicable aux opérateurs d'importance vitale

Le « sous-secteur » du transport maritime et fluvial est ainsi rattaché au secteur du transport qui est l'un des douze secteurs d'importance vitale retenus dans le cadre du dispositif interministériel de sécurité des activités d'importance vitale (SAIV), inscrit dans le code de la défense.

L'article 22 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019, mise en application par le décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale, impose aux acteurs identifiés comme opérateurs d'importance vitale (OIV), le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent.

Pratiquement, l'arrêté du 11 août 2016 fixe les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transports maritime et fluvial ». Les OIV du secteur maritime doivent identifier leurs Systèmes d'information d'importance vitale (SIIV), leur appliquer les mesures de sécurité de l'arrêté sectoriel dans les délais prévus par ce même arrêté et déclarer à l'ANSSI de façon immédiate les incidents SSI affectant de manière significative leurs SIIV.

1.1.2.2 Cadre réglementaire aux opérateurs de services essentiels

Le « sous-secteur » du transport par voie d'eau est rattaché au secteur du transport qui est l'un des sept secteurs de la directive SRI / NIS et l'un des 15 secteurs de sa transposition française.

La directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite Directive SRI ou NIS, crée un cadre réglementaire pour renforcer la cybersécurité des opérateurs de services qui sont essentiels (OSE) au fonctionnement de l'économie et de la société.

Elle vise ainsi à harmoniser les capacités nationales de cybersécurité ainsi qu'à renforcer la collaboration transfrontalière et la surveillance des secteurs critiques à travers l'UE. Ses considérants 10 et 11 sont spécifiques au secteur maritime : « Les exigences de sécurité pour les entreprises, les navires, les installations portuaires, les ports et les services de trafic maritime en vertu des actes juridiques de l'Union couvrent toutes les opérations, y compris les systèmes de radio et de télécommunication, les systèmes et réseaux informatiques » et « lors de l'identification des opérateurs « de services essentiels » dans le secteur des transports par eau, les États membres devraient tenir compte des codes et lignes directrices internationaux

existants et futurs élaborés en particulier par l'Organisation maritime internationale, en vue de fournir aux opérateurs maritimes individuels une approche cohérente ».

Les opérateurs de services essentiels identifiés dans l'écosystème du transport par eau (en dehors du sous écosystème fluvial) sont les suivants :

- les entreprises de transport maritime et côtier de passagers et de marchandises, telles que définies pour le transport maritime à l'annexe I du règlement (CE) 725⁄2004 ;

- les organismes de gestion des ports, y compris leurs installations portuaires (définies comme « un endroit où l'interface navire/port a lieu ; cela comprend des zones telles que les mouillages, les postes d'amarrage et les approches depuis la mer, selon le cas » dans le règlement (CE) 725⁄2004) et les entités exploitant des infrastructures et équipements contenus dans les ports ;

- les exploitants de services de trafic maritime (définis comme « service conçu pour améliorer la sécurité et l'efficacité du trafic maritime et pour protéger l'environnement, qui a la capacité d'interagir avec le trafic et de répondre aux situations de trafic qui se développent dans la zone des STM » dans la Directive 2002⁄59 /CE).

La directive SRI / NIS a été transposée en France via la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité qui fixe le cadre général, le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique qui fixe les modalités de désignation des OSE et la liste des services essentiels, et par l'arrêté du 14 septembre 2018 qui fixe les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018.

La directive SRI / NIS s'applique aux grands ports maritimes français et concerne, par ailleurs, les compagnies maritimes. Sur le modèle de la loi de programmation militaire, la directive SRI / NIS impose aux OSE d'identifier leurs systèmes d'information essentiels (SIE), de leur appliquer les mesures de sécurité dans les délais prévus et de déclarer à l'ANSSI les incidents SSI affectant de manière significative leurs SIE.

Il convient enfin de rappeler qu'en 2019, le règlement sur la cybersécurité de l'UE renforce la position de l'ENISA dans les questions de cybersécurité pour les États membres de l'UE et définit un cadre de certification de cybersécurité à l'échelle de l'UE pour les produits, services et processus TIC. Ce cadre fournira un ensemble complet de règles, d'exigences techniques, de normes et de procédures afin d'attester que les produits et services TIC peuvent être fiables sur la base des exigences de l'UE.

1.1.3 Cadre réglementaire de la « protection des données portuaires »

Les conventions SOLAS (« sauvegarde de la vie humaine en mer ») et FAL (« facilitation du trafic maritime international ») définissent huit formulaires normalisés à utiliser pour échanger des informations au sein de l'écosystème maritime, en particulier entre le port et des tiers :

- Formulaire FAL n° 1 « déclaration générale »

- Formulaire FAL n° 2 « déclaration de la cargaison »

- Formulaire FAL n° 3 « déclaration des provisions de bord »

- Formulaire FAL n° 4 « déclaration des effets et marchandises de l'équipage »

- Formulaire FAL n° 5 « liste de l'équipage »

- Formulaire FAL n° 6 « liste des passagers »
- Formulaire FAL n° 7 « marchandises dangereuses »
- Déclaration maritime de santé

L'échange électronique des informations requises est obligatoire depuis le 9 avril 2019, notamment à l'aide de systèmes de « guichet unique » déployés par les pouvoirs publics. Cette standardisation des échanges de données a un fort impact sur les écosystèmes informatiques portuaires et pose de nouveaux défis de sécurité informatique.

La cybersécurité, en particulier pour les navires, n'est abordée directement au niveau international que depuis 2017 grâce à des directives et recommandations à l'écosystème maritime mondial.

L'Organisation Maritime Internationale (OMI), via son Comité de facilitation (FAL) et son Comité de la sécurité maritime (MSC) ont défini les lignes directrices de l'OMI sur la gestion des cyberrisques maritimes dans une circulaire MSC-FAL.1/Circ. 3 du 5 juillet 2017. Y est reconnu l'urgence de sensibiliser aux menaces et aux vulnérabilités liées aux cyberrisques et de fournir des recommandations de haut niveau sur la gestion des cyberrisques maritimes contre les cybermenaces et vulnérabilités actuelles et émergentes, y compris les principaux domaines qui soutiennent une gestion efficace des cyberrisques (identifier, protéger, détecter, répondre et récupérer).

Ces directives font la distinction entre les systèmes informatiques (utilisation des données comme informations) et les systèmes industriels (utilisation des données pour contrôler ou surveiller les processus physiques). Elles reconnaissent que toutes les organisations de l'industrie du transport maritime sont différentes et doivent se référer aux exigences des gouvernements membres et des administrations de pavillon ainsi qu'aux normes et meilleures pratiques internationales ou industrielles pertinentes (par exemple, NIST Framework, ISO/IEC 27001) afin d'assurer la sécurité la plus pertinente.

La directive 2010/65/UE du 20 octobre 2010 concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres (remplacée par le règlement 2019/1239 du 20 juin 2019 qui ne rentrera en vigueur qu'en 2025) exige que les ports des États membres acceptent des formulaires standardisés (formulaires FAL) afin de faciliter le trafic. Cette directive introduit également les systèmes SafeSeaNet établis au niveau national et au niveau de l'Union européenne pour faciliter l'échange sécurisé de données entre les autorités maritimes des États membres et les systèmes d'autres autorités (par exemple, les systèmes douaniers).

Sous l'impulsion du ministère chargé des ports, un projet de simplification et de digitalisation de la transmission des formalités applicables aux navires a été mené au cours des dernières années : le « guichet unique maritime et portuaire » (GUMP).

Ce guichet a été progressivement mis en place depuis 2010, conformément aux prescriptions de la directive (UE) 2010/65. La France a, pour sa part, décidé de mettre en place un système d'information centralisé reposant sur les différents systèmes d'informations portuaires (SIP). La solution déployée permet ainsi la saisie et la transmission de données dématérialisées fournies par les déclarants dans les SIP vers les systèmes d'information des administrations françaises et européennes.

Le secteur portuaire, comme tous les secteurs économiques, est enfin directement concerné par les exigences pour la protection des données personnelles fixées par le règlement (UE) 2016/679 du 27 avril 2016 relatif à protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données, dit Règlement général sur la protection des données (RGPD). Des exigences pleinement intégrées dans les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

1.2 Infrastructures et services portuaires

Les infrastructures et services portuaires présentent une grande diversité d'un port à l'autre : au fil des années, les ports maritimes ont adapté leurs infrastructures et services aux spécificités géographiques et territoriales locales, aux activités liées à la l'emplacement du port (bassins de pêche existants autour, un emplacement idéal pour le tourisme, un emplacement au carrefour de différents pays et continents, etc.) et aux différents défis auxquels les ports doivent faire face.

L'infrastructure globale d'un port est composée d'infrastructures marines (brise-lames, dragage, écluses, bassins, jetées, quais, jetées d'amarrage, etc.), d'infrastructures de distribution (routes internes, voies ferrées, passerelles, etc.), de bâtiments et de terminaux gérés et maintenu par l'administration portuaire. Les installations portuaires sont généralement louées par l'autorité portuaire à des exploitants de terminaux privés chargés de gérer et d'entretenir la superstructure (comme les grues, les silos, les clôtures spécifiques, les installations de contrôle, les terminaux de passagers) pour effectuer les opérations spécifiques des installations portuaires.

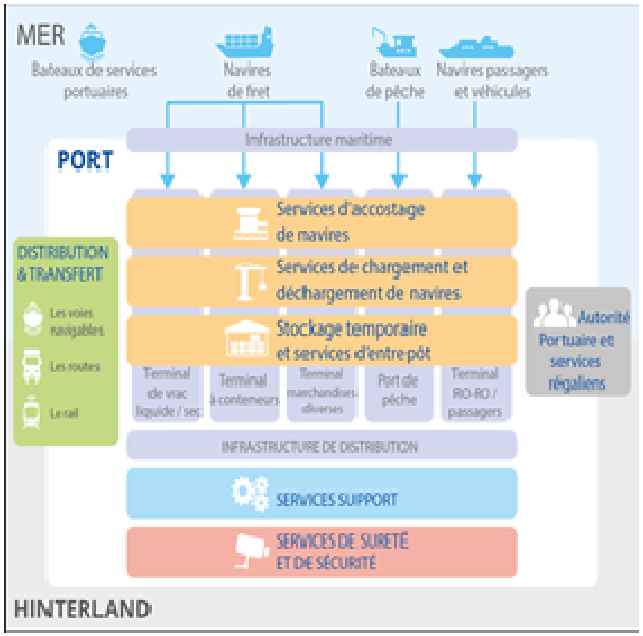
En outre, diverses autorités résident dans les installations portuaires pour fournir des services, des contrôles et des inspections liés aux opérations des navires et des ports (voir 3.3).

Un port maritime peut s'adresser à quatre grandes catégories d'activités auxquelles les infrastructures et les services sont adaptés :

- activités liées au fret maritime (conteneur, cargaison générale, vrac liquide ou sec, etc.) avec une infrastructure et des services dédiés pour accueillir les cargos et gérer les opérations connexes (par exemple, déchargement et chargement, stockage, inspection douanière, contrôles sanitaires, etc.) ;
- activités liées au transport de passagers (ferries et navires de croisière) et de véhicules avec des infrastructures et des services dédiés pour accueillir les passagers et les véhicules à bord des navires et les opérations liées aux gestionnaires (par exemple, passerelles pour passagers, parking, restaurants et bars, contrôle aux frontières, etc.). Cela comprend l'activité RoRo (Roll-on / roll-off ship) car la cargaison est sur des camions ;
- activités liées à la réparation des navires ;
- activités liées à la pêche avec des infrastructures et des services dédiés pour accueillir les bateaux de pêche et gérer les opérations connexes (par exemple, déchargement / chargement du poisson, inspection du poisson, stockage réfrigéré du poisson, etc.).

Afin de soutenir ces différentes activités, le port fournit les principaux services, représentés sur la figure 2 et détaillés dans le tableau 1.

Figure 2 : Infrastructures et services portuaires (source ENISA)



Ces services sont regroupés en sept catégories, qui ont été définies sur la base des recherches documentaires et des informations fournies par les experts qui ont contribué à ce guide.

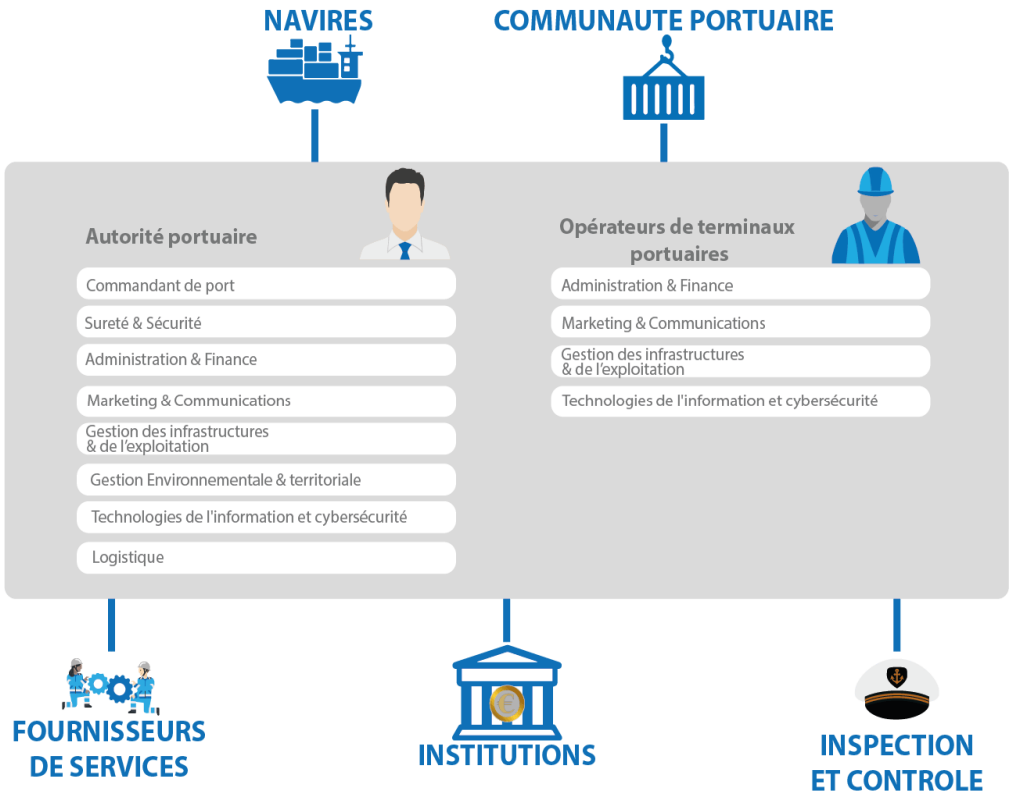
Tableau 1 : Services portuaires détaillés

Catégorie de service	Description du service
Services d'accostage des navires	Lorsqu'un navire arrive et quitte un port, différents services sont fournis : attribution des postes d'amarrage, pilotage maritime, fournitures de navires telles que le ravitaillement en carburant ou l'approvisionnement alimentaire, remorquage, amarrage, gestion de la sécurité et de la sûreté des navires, gestion de l'eau en vrac, services à l'équipage , réparation de navires, etc.
Services de chargement et de déchargement de navires	Lorsqu'un navire est amarré dans un port, différents services sont fournis pour charger et décharger du fret, des poissons, des passagers et des véhicules : opérations de grues de quai et de bandes transporteuses, pompage, suivi du fret, passerelles de passagers mise en place, contrôles d'accès à l'embarquement, sûreté et sécurité, surveillance des opérations, etc.
Services de stockage et de séjour temporaires	Lorsque le fret ou les poissons sont sur les quais, des services de stockage temporaire sont fournis avant leur distribution et leur transfert, selon la nature du fret : déplacement, stockage et empilement de conteneurs ; exploitation et stockage de bandes transporteuses de solides en vrac ; convoyeurs à grains et silos ; pompage de liquides en vrac et remplissage de réservoirs ; stockage de marchandises générales ; stockage réfrigéré de marchandises ; etc. De manière similaire, les services de séjour sont fournis pour les véhicules et les passagers : parking, salons passagers, installations de manutention des bagages, restaurants et bars, centres commerciaux, etc.
Services de distribution et de transfert	Pour assurer la connectivité avec l'arrière-pays, des services de distribution et de transfert sont fournis : services portuaires intérieurs, gares et gares de triage, contrôles des passagers et des bagages, plates-formes de transport intermodal, contrôle des conteneurs, entrée et sortie du port, etc.
Services d'assistance	Pour soutenir les services décrits ci-dessus, l'autorité portuaire ou d'autres sociétés privées fournissent le service suivant : suivi du fret, contrôle du trafic maritime, gestion des terres et des infrastructures, gestion des biens immobiliers et des installations, gestion des opérations terminales, gestion de l'accostage et du pilotage, gestion des marchandises dangereuses, maintenance, gestion des opérations portuaires, administration portuaire, etc.
Services de sécurité et de sûreté	Pour protéger les infrastructures, les services et les personnes qui travaillent et traversent le port, des services de sûreté et de sécurité sont équipés pour prévenir les accidents ou les activités malveillantes telles que le terrorisme : caméras et surveillance radar, contrôles d'accès, alarmes, signaux, détections, etc.
Services régaliens	Des services régaliens peuvent être situées dans les installations portuaires pour fournir divers services, notamment des contrôles et inspections : douanes, police, garde-côtes, pompiers, contrôle par l'État du port, sécurité civile, sauvetage en mer, santé, sécurité de la navigation, prévention de la pollution, hygiène et contrôles vétérinaires, contrôles des captures de poissons, etc.

1.3 Principaux acteurs portuaires

Le panorama des principaux acteurs portuaires impliqués dans les opérations et les processus portuaires est complexe et est accentué par les différences considérables de gouvernance et de fonctionnement qui peuvent exister entre les ports. Cependant, un aperçu peut être établi pour différencier les catégories de parties prenantes par macro-rôles.

Figure 3 : Aperçu des acteurs portuaires (source ENISA)



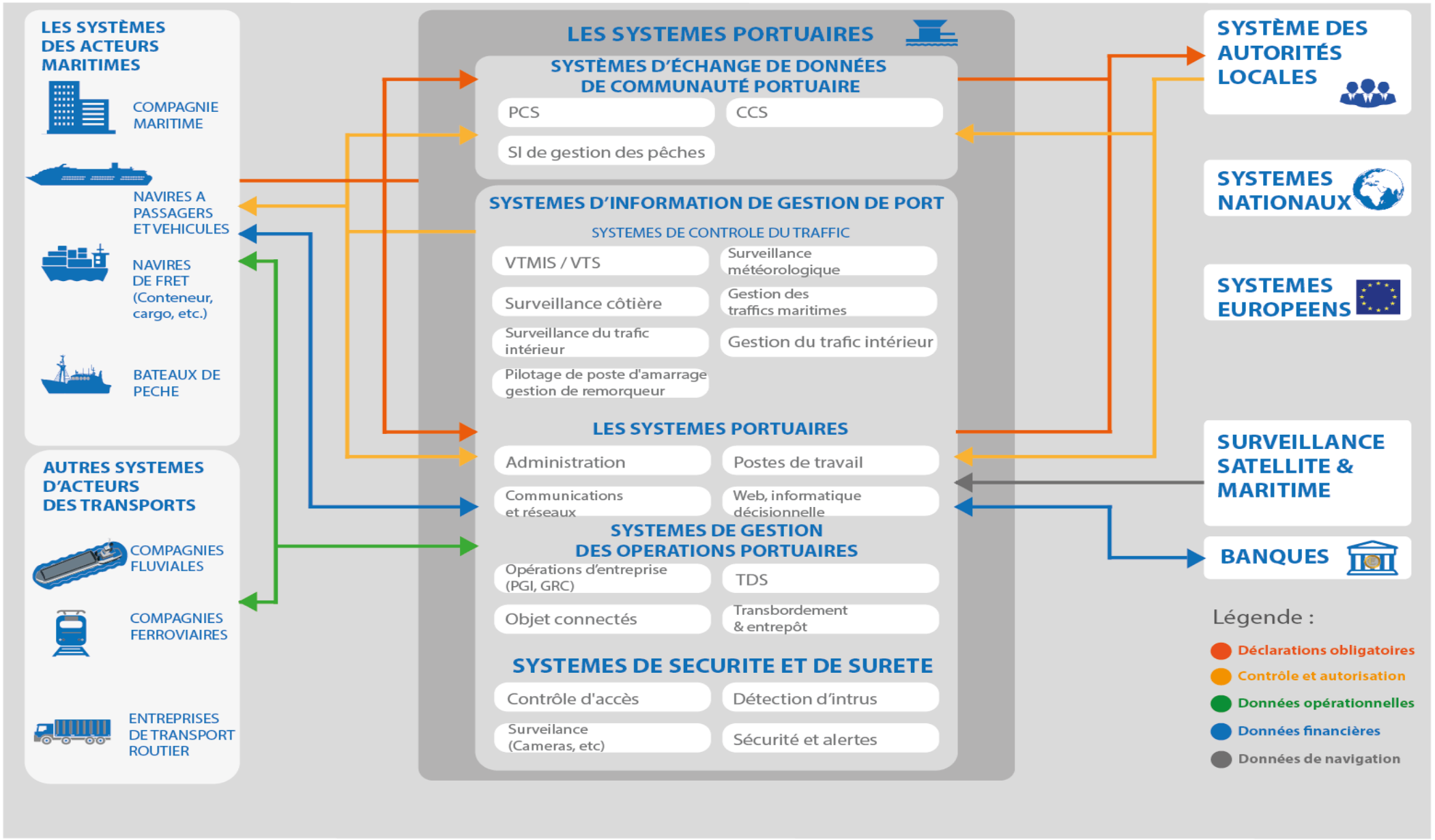
1.4 Modèle de référence

La complexité et la diversité de l'écosystème portuaire (divers modèles opérationnels et économiques, gouvernance différente, grande typologie des acteurs impliqués, responsabilités partagées entre les acteurs, etc.) et l'unicité de chaque port se reflètent dans une approche très diversifiée de l'information et de l'exploitation gestion des systèmes technologiques (IT / OT). En effet, d'un port à un autre, les systèmes informatiques et industriels ne sont pas les mêmes, ne sont pas exploités et gérés par les mêmes types de parties prenantes et ne sont pas mis en œuvre de la même manière.

Ce guide fournit un modèle de référence basé sur celui établi par l'ENISA. Ses objectifs sont de répertorier les principaux systèmes portuaires, les flux de données et les interactions avec les systèmes externes.

Cependant, ce modèle doit être nuancé et adapté, car il ne peut pas correspondre pleinement aux spécificités de chaque port. Par exemple, la fonctionnalité du système de communauté portuaire diffère entre les ports, en fonction de leurs activités et services spécifiques ainsi que de leurs autorités de supervision.

Figure 4 : Modèle de référence des systèmes portuaires (source ENISA)



1.4.1 Description des systèmes

Le modèle de référence représente les systèmes portuaires (bloc au milieu) et les systèmes tiers interagissant avec eux.

Les systèmes des tiers sont regroupés en quatre catégories principales :

- les systèmes utilisés par les acteurs maritimes (compagnies maritimes, agent maritime, capitaine et équipage des navires, etc.) ;
- les systèmes utilisés par d'autres acteurs du transport pour partager des informations sur le fret ou les passagers et permettre le transbordement (entreprises de transport par voie navigable, sociétés de voirie, sociétés ferroviaires, etc.) ;
- les systèmes utilisés par les autorités aux niveaux local, national et européen ;
- les systèmes utilisés pour la surveillance par satellite et maritime.

Concernant les systèmes portuaires, ils sont regroupés en deux grandes catégories :

- les systèmes d'échanges de données de la communauté portuaire pour les services liés aux navires, au fret, notamment utilisés comme point central pour l'échange de données avec les compagnies maritimes (exemple des PCS, qui composent le guichet unique maritime et portuaire) ;
- les systèmes d'information de gestion portuaire, qui comprennent les systèmes de contrôle du trafic maritime, les systèmes d'entreprise (courriels, ERP, etc.), les systèmes de sécurité et de sûreté ainsi que les systèmes de gestion des opérations des terminaux, souvent détenus par des entreprises privées.

1.4.2 Description des flux de données

Les systèmes portuaires interagissent avec une large gamme de systèmes via des interconnexions de machine à machine ou manuelles (avec des informations échangées via des interfaces Web, par appels téléphoniques, e-mails, papier ou fax).

Une grande quantité de données est échangée entre le port et les différents intervenants, qui est classée en cinq catégories selon ce modèle de référence :

- les déclarations obligatoires (informations que les compagnies maritimes ou autres parties prenantes doivent signaler à l'autorité portuaire ou à d'autres autorités, en ce qui concerne les législations internationales, européennes et nationales) ;
- le contrôle et l'autorisation accordés par les autorités aux acteurs commerciaux (par exemple autorisation d'accès au port, autorisation de déchargement des marchandises) ;
- les données opérationnelles liées aux services et processus portuaires (par exemple, les besoins de ravitaillement des navires, la programmation des opérations de fret) ;
- les données financières (par exemple, facturation du port à son client, paiement) ;
- les données de navigation (par exemple, la position GPS d'un navire dans la zone portuaire, les données AIS).

2. IDENTIFIER LES ACTIFS PORTUAIRES

Pour identifier les cybermenaces associées à l'écosystème portuaire, il est essentiel de partir de l'identification et de la répartition des actifs du port. La figure 5 (source ENISA) donne un aperçu des principales catégories d'actifs que l'on peut trouver dans un port et détaille les actifs de chaque catégorie : cette taxonomie ne doit pas être considérée comme exhaustive ; elle vise à représenter les principaux atouts et ne reflète pas la diversité et les spécificités des différents ports. Le tableau 3 décrit chaque actif représenté dans la taxonomie des actifs.

Dix catégories d'actifs ont été identifiés au niveau européen : l'infrastructure fixe, l'infrastructure mobile, les systèmes et réseaux industriels, les appareils terminaux industriels associés, les systèmes informatiques, les composants réseaux et communications, les systèmes de sûreté et de sécurité, les informations et données, et les personnes.

Figure 5 : Classement (source ENISA)

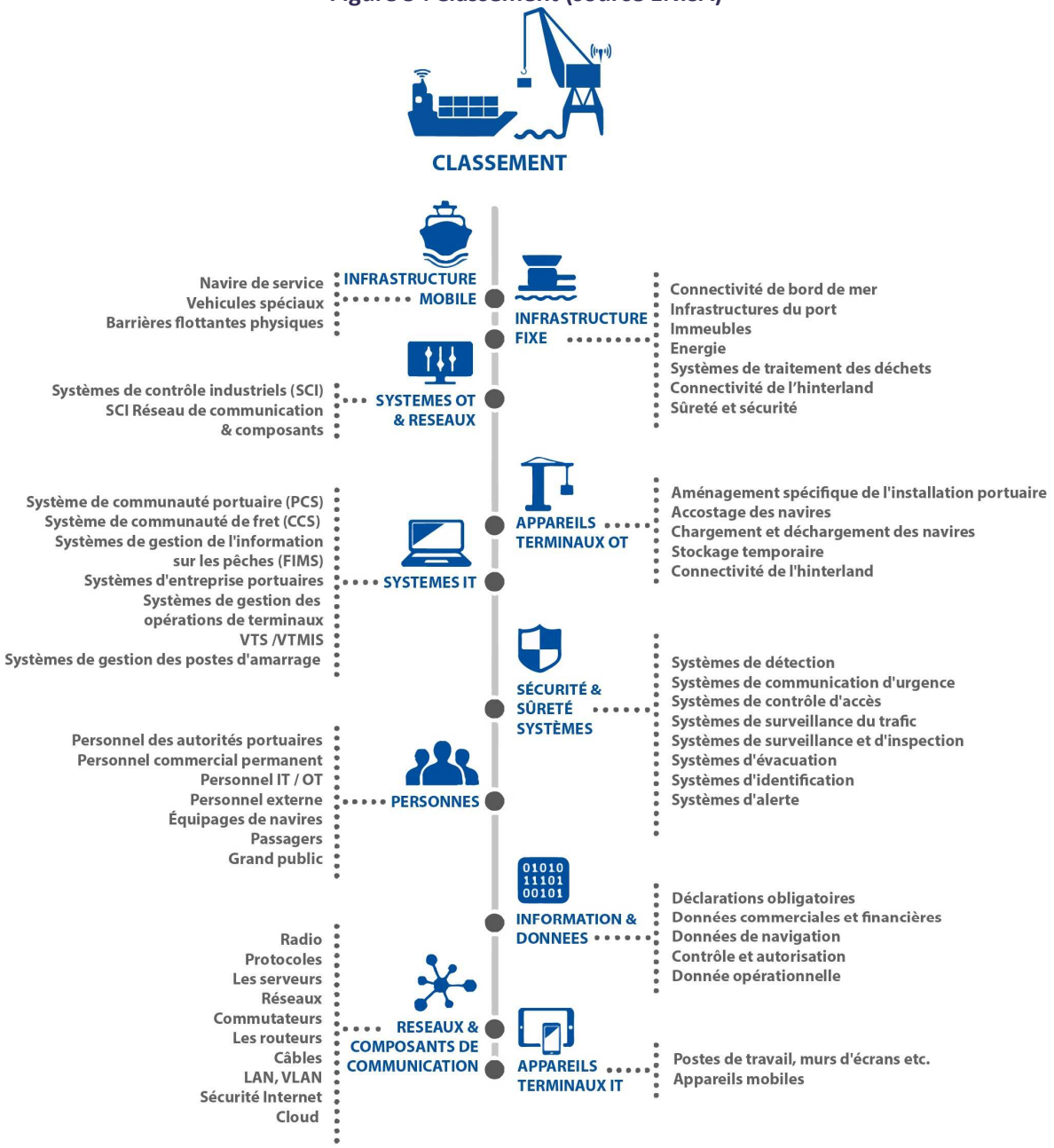


Tableau 3 : Description des actifs du port

Sous-catégories	Description
Infrastructures fixes	
Connectivité maritime	Actifs liés à la navigation entre le bord de mer et la zone portuaire pour garantir que les navires peuvent entrer et sortir du port : brise-lames, écluses de mer, bouées, balises lumineuses, marquage des voies navigables, marée, surveillance du vent et des courants, surveillance radar des cours d'eau.
Infrastructure portuaire	Actifs liés à l'amarrage des navires dans le port (quais, quais, jetées, jetées), l'éclairage, le contrôle d'accès (portails, systèmes de lecture de plaques, détecteurs) et le transport à l'intérieur des zones portuaires (routes, chemins de fer, voies navigables, chemins piétonniers).
Bâtiments	Bâtiments portuaires hébergeant les différents bureaux liés aux services portuaires (bureau du maître de port, bureau de douane, etc.) et centres de données hébergeant tous les systèmes informatiques et OT.
Energie	Actifs liés à la fourniture d'énergie pour l'écosystème portuaire (bâtiments, navires, etc.) : réseau électrique (à haute tension pour les grands ports), soutage et stations de livraison d'eau douce, canalisation, carburant, essence, etc.
Systèmes de traitement des déchets	Déchets gérés par le port mais également déchets des navires (déchets solides tels que plastique, papier, verre, déchets alimentaires et liquides tels que eaux de cale, boues et eaux usées).
Connectivité de l'hinterland	Atouts de connectivité de l'arrière-pays dont dispose le port, en tant qu'interface entre la mer et les systèmes de transport de l'arrière-pays, tels que les gares et les systèmes de chargement et d'expédition du matériel roulant, les infrastructures routières, les stations intermodales, les canaux et les infrastructures portuaires reliant les voies navigables intérieures.
Sûreté et sécurité	Infrastructures dédiées à la sûreté et à la sécurité : tour de contrôle, salle d'opération, centre de sécurité, installations de premiers secours (lutte contre l'incendie, pollution, confinement, voies d'évacuation, installations médicales, etc.).
Infrastructures mobiles	
Navires de service portuaires	Navires dédiés à la fourniture des services spécifiques sur l'eau aux navires : bateaux-pilotes, remorqueurs, aide à l'embarcation et à l'amarrage, navires de ravitaillement, navires de sécurité, navires d'inspection et de sécurité.
Véhicules spéciaux	Véhicules du port dédiés pour fournir des services intérieurs: lutte contre les incendies, ambulance, unités mobiles de contrôle du fret, etc.
Barrières flottantes physiques	Barrières flottantes physiques utilisées par le port pour protéger d'autres navires et zones portuaires critiques, pour contenir les pollutions et d'autres usages, le port peut utiliser.

Systèmes et réseaux industriels	
Systèmes de contrôle industriel (ICS)	Systèmes permettant de gérer l'accès au port et l'accostage des navires (ponts, écluses, portes, etc.), l'infrastructure portuaire (bâtiments, etc.), les opérations terminales (grues, stockage, etc.) et composés des composants suivants : automates et analyseurs (contrôleurs logiques programmables « PLC », unité terminale distante « RTU »), bases de données (Historian, MES (Système d'Exécution de la Fabrication), etc.), systèmes de supervision (système de contrôle distribué « DCS », contrôle de supervision et acquisition de données « SCADA »), interface homme-machine « IHM » / postes de travail (consoles de programmation, poste de travail d'ingénierie), systèmes de maintenance et systèmes instrumentés de sécurité (SIS)
Réseaux et composants de communications ICS	Actifs gérés par le port pour assurer les communications entre les composants ICS : commutateurs (gérés et non gérés), points d'accès sans fil, protocoles, systèmes d'alimentation (eau, électricité, etc.)
Dispositifs OT END	
liés à un aménagement spécifique de l'installation portuaire	Dispositifs terminaux de l'ICS liés à l'aménagement spécifique de l'installation portuaire : clôture spécifique et contrôle d'accès, équipement de sûreté et de sécurité spécifique, équipement de première intervention, salle opérationnelle spécifique, etc.
liés à l'accostage des navires	Dispositifs terminaux de l'ICS liés à l'accostage des navires portuaires : le bateau, les systèmes de gestion des postes d'amarrage, les équipements spécifiques d'inspection et de contrôle, etc.
liés au chargement et au déchargement des navires	Dispositifs terminaux OT utilisés pour charger et décharger les navires : équipements et systèmes de manutention spécifiques au terminal (grues, rampes pour passagers, pipelines, tapis, convoyeurs, etc.), suivi du fret spécifique aux terminaux systèmes (codes à barres, compteurs de liquide, identification par radiofréquence « RFID », scellés, balances, etc.), scanners de badges ou de billets, systèmes de lecture de plaques, détecteurs de défauts dans les systèmes de chargement / déchargement automatisés (fuites, chocs, bourrage, etc.)
liés au stockage temporaire	Dispositifs terminaux OT utilisés une fois la cargaison ou les conteneurs hors du navire, et temporairement stockés dans les zones portuaires : systèmes de transport interne (chariot enjambeur, cour, camion, châssis, etc.), systèmes d'équipement de stockage (rayonnages à palettes, tankage, etc.), des magasins réfrigérés et non refroidis, des silos, des réservoirs, des interrupteurs (gérés et non gérés) pour les tuyaux et les bandes transporteuses, des points d'accès sans fil pour les scellés «intelligents» et les dispositifs d'auto-localisation des conteneurs, etc.
liés à la connectivité avec l'hinterland, le fret, les conteneurs, les véhicules ou les passagers	Dispositifs terminaux utilisés pour contrôler le fret, les conteneurs, les véhicules ou les passagers et les inspecter, puis les transporter vers d'autres systèmes de transport : systèmes de contrôle et d'inspection (scanners, systèmes d'inspection, rayons X), gare ferroviaire, gares de triage des wagons, plates-formes de transport multimodal pour les personnes (passagers, travailleurs, etc.), installations portuaires intérieures, équipements de contrôle des portes portuaires (lecture de plaques, badges, lecture de codes-barres, détecteurs)

Systèmes informatiques	
Port Community System (PCS)	Système, généralement détenu et géré par l'autorité portuaire ou les parties prenantes du port, de plus en plus organisé, comme un système de guichet unique pour partager les informations sur les opérations portuaires liées aux navires entre toutes les parties prenantes du port (date d'arrivée ou de départ du navire données par les compagnies maritimes, déclarations obligatoires telles que la liste de l'équipage, les déclarations de marchandises dangereuses, les réservations de services de navire, etc.). Ils visent à faciliter la gestion des escales des navires au moyen de la digitalisation des formalités administratives.
Cargo Community System (CCS)	Système, généralement détenu et géré par les parties prenantes du port qui sont généralement des sociétés privées en charge des opérations du terminal portuaire, permettant de partager des informations sur les opérations portuaires liées aux marchandises, à la cargaison et aux conteneurs entre tous les acteurs impliqués (contenu de la cargaison, localisation d'un conteneur, heure de son transfert, déclarations en douane, etc.).
Systèmes d'entreprise portuaires	Systèmes composés de différentes applications, systèmes, postes de travail et serveurs, communs à toutes les entreprises : finances, ressources humaines (RH), systèmes de communication et de réseaux, systèmes d'e-mailing, systèmes de vente et de marketing (ERP), etc. Systèmes de gestion des opérations de terminaux Les systèmes de gestion des opérations de terminaux, généralement détenus, utilisés et entretenus par des opérateurs de terminaux privés, sont principalement composés de différents systèmes: des systèmes d'exploitation d'entreprise pour planifier et gérer la logistique et les opérations (ERP, CRM, etc.), les systèmes industriels spécifiques aux opérations des terminaux (grues, etc.), les systèmes d'exploitation des terminaux (TOS) utilisé pour optimiser les systèmes de logistique, de transbordement et de stockage.
Suivi du trafic maritime (VTS) / Système d'Information de Gestion du Trafic des Navires (VTMIS)	Systèmes de surveillance du trafic maritime (pour le VTS), intégrant le cas échéant par extension (VTMIS) d'autres informations et fonctionnalités pour augmenter l'efficacité des opérations portuaires (allocation des ressources, etc.).
Systèmes de gestion des postes d'amarrage	Systèmes utilisés par les autorités portuaires pour gérer et assurer la sécurité des processus d'amarrage: avertissements et alertes, données météorologiques, flux de caméras vidéo, gestion de l'attribution des postes d'amarrage, etc.
Appareils IT END	
Postes de travail des terminaux informatiques	Différents postes de travail sont utilisés dans les ports : systèmes informatiques dédiés aux systèmes industriels, à la maintenance, aux postes mobiles et fixes, etc.
Appareils mobiles	Différents appareils mobiles sont utilisés dans les ports : smartphones, tablettes, radios terrestres à ressources partagées « TETRA », appareils spécifiques utilisés pour la logistique (numérisation, etc.) etc.

Réseaux et composants de communication	
Radio	Systèmes radio (identification par radiofréquence « RFID », VHF, etc.) utilisés pour de nombreux processus portuaires : communication avec les navires, opérations de sûreté et de sécurité, gestion logistique, etc.
Protocoles	Protocoles utilisés pour échanger des informations : EDI, API, protocoles d'authentification , etc.
Serveurs	Serveurs utilisés dans les ports pour différentes finalités : serveurs Web, serveurs d'applications, serveurs proxy, serveurs de messagerie, serveurs virtuels, imprimantes, etc. Réseaux Différents réseaux sont installés dans les ports : radios VHF (Internet, WiMAX / WIFI, Satellite, réseaux ad-hoc, VLAN / LAN, etc. Ils peuvent être gérés par différentes parties prenantes à différents niveaux.
Commutateurs, routeurs, concentrateurs	Composants utilisés pour transmettre des paquets de différentes manières entre différents réseaux.
Sécurité du réseau	Systèmes de protection du réseau, pare-feu, IPS / IDS, infrastructure à clé publique « PKI » / authentification multifacteur « MFA », antivirus, information sur la sécurité et gestion des événements « SIEM » et d'autres solutions de sécurité sont installés dans les zones portuaires.
Cloud	Solutions cloud pour héberger certaines données, par exemple des e-mails et partager des fichiers.
Informations et données	
Déclarations obligatoires	Déclarations obligatoires pour qu'un navire pénètre dans la zone portuaire, conformément aux réglementations internationales, européennes, nationales et locales. Par exemple, obligatoire par la Convention FAL : passagers et équipage, navire, fret, contrôle aux frontières, déchets, sécurité, santé, informations sur les voyages sont requis.
Données commerciales et financières	Comme toute entreprise, les ports fournissent des services aux entreprises (compagnies maritimes, etc.) et réservent différents services à leurs prestataires (prestataires ICT par exemple) : financiers et commerciaux sont des échanges (transfert d'argent, facturation, etc.).
Données de navigation	Grâce aux données satellitaires et de navigation (AIS, SafeSeaNet, etc.), les différentes parties prenantes partagent les données de navigation avec le port (position GPS, informations sur les routes maritimes, etc.).
Contrôle et autorisation	Les autorités portuaires et d'autres autorités nationales contrôlent et délivrent l'autorisation de mouvement des navires et des cargaisons.
Données opérationnelles	Afin de planifier et de gérer tous les services (services maritimes, services logistiques, etc.), des données opérationnelles sont partagées entre les acteurs portuaires.

Systèmes de sûreté et de sécurité	
Systèmes de contrôle d'accès	Portails automatiques, systèmes de clôtures intelligentes, systèmes de badges, systèmes de surveillance et de comptage des accès.
Systèmes de détection	Vidéoprotection, systèmes de gestion des incidents, systèmes de centre de première intervention, IDS (systèmes de détection d'intrusion), des systèmes de détection des comportements anormaux.
Systèmes de surveillance du trafic	Systèmes de surveillance radar et électro-optique, les systèmes de surveillance de la circulation des trains et des camions.
Systèmes de surveillance et d'inspection	Personnel de surveillance et de gardiennage, équipes cynotechniques, patrouilles véhiculées, détecteurs (incendies, fuites de gaz, nucléaire, etc.), scanners à rayons X.
Systèmes d'identification et d'authentification	Systèmes biométriques, terminaux portables de contrôle d'identité, reconnaissance faciale.
Systèmes d'alerte	Sirènes et haut-parleurs.
Systèmes d'évacuation	Guidage de sortie, points de rassemblement, écrans de guidage, portes de secours.
Systèmes de communication d'urgence	
Personnes	
Personnel de l'autorité portuaire	Personnels permanents ou temporaires, statuaires ou contractuels, employés par l'autorité portuaire.
Personnel commercial permanent	Personnels des sociétés opérant en permanence dans les ports emploient des personnes, en tant que personnel statuaire (opérateurs de terminaux, prestataires de services permanents, etc.).
Personnel informatique / OT	Personnels employés par les autorités portuaires et les entreprises privées, opère dans différents systèmes pour mettre en place de nouvelles solutions et les maintenir (RSSI, CIO, administrations, etc.).
Personnel externe	Personnels externes des installations portuaires, autre personnel de service (tiers), personnel temporairement autorisé (entrepreneurs, chauffeurs de taxi, etc.).
Équipages de navires	Lorsqu'un navire arrive dans un port, les membres de l'équipage et leur capitaine peuvent utiliser les différentes installations du port (restaurant, bar, etc.).
Passagers	Passagers qui traversent les zones portuaires pour monter dans les navires de croisière et les ferries.
Grand public	Généralement, certaines zones portuaires sont ouvertes au public (tourisme, recherche, etc.).

3. CARTOGRAPHIER LES CYBERMENACES ET LES ENJEUX DE CYBERSÉCURITÉ

3.1 Diversité des cybermenaces

Les ports sont confrontés à de nombreuses cybermenaces et enjeux de cybersécurité, certains d'entre eux sont assez génériques dans n'importe quel environnement informatique et OT, tandis que d'autres sont assez spécifiques aux écosystèmes portuaires.

En l'espèce une cyber-attaque va porter atteinte selon les cas à la disponibilité, à la confidentialité ou à l'intégrité des données :

- **disponibilité** : propriété d'être accessible et utilisable à la demande par une entité autorisée (ex. : le brouillage, d'un GPS par exemple, le rançonnement ou le déni de service sont deux types d'attaques qui visent à rendre indisponibles les données à des fins d'extorsion dans le cas des logiciels de rançonnement) ;

- **confidentialité** : propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés (ex. : la perte de confidentialité peut se produire à chaque fois qu'une intrusion se produit dans un système traitant ou stockant des informations de nature confidentielle, comme des données commerciales ou des secrets industriels) ;

- **intégrité** : garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime (de nombreux types d'attaque ont pour résultat la corruption, c'est-à-dire la perte d'intégrité, des données ; le leurrage du GPS est un exemple de perte d'intégrité des données - des données erronées sont traitées par le système).

Le tableau 3 identifie l'impact possible des incidents de cybersécurité pour un port.

Tableau 3 – Impacts possibles pour un port (source : ENISA)

	Impacts	Description
	**Arrêt des opérations, paralysie portuaire**	L'arrêt des opérations portuaires est un impact très redouté par l'écosystème portuaire : s'il dure plus de quelques heures, il peut nuire fortement aux opérations commerciales (perte d'argent), à la livraison de biens essentiels pour une nation, en particulier pour les îles (nourriture, carburant, etc.) et posent des problèmes de sûreté et de sécurité (attente de plusieurs navires à l'entrée du port).
	**Blessures ou décès humains, enlèvement**	Les ports doivent faire face à des défis de sécurité et de sûreté élevés, car de nombreuses personnes travaillant dans les zones portuaires peuvent effectuer des travaux dangereux (manipulation de grues, de marchandises dangereuses, etc.) et parce que les ports doivent également gérer facilement un flux de passagers assez important à prévoir (ferries, grands bateaux de croisière, etc.).
	**Vol de données sensibles et critiques**	Les systèmes portuaires peuvent contenir des informations critiques, qu'il s'agisse d'informations personnelles (données d'équipage ou de passagers), d'informations commerciales critiques (emplacement et contenu des conteneurs, savoir-faire concurrentiel) ou d'informations de sécurité nationale (le port étant un atout essentiel pour un nation) : le vol de ces informations peut avoir des conséquences désastreuses.
	**Vol de marchandises**	Les attaquants peuvent parcourir les listes de marchandises et de conteneurs pour identifier les marchandises les plus précieuses pour les marchés noirs (à voler dans le port ou à cibler pour de futures attaques de piraterie lorsque le navire est en mer).
	**Trafic illégal**	L'écosystème marin est l'un des plus grands terrains de jeu du crime organisé : les ports sont souvent utilisés pour le trafic illégal et criminel (drogues, armes, marchandises interdites, personnes les plus recherchées, etc.).
	**Pertes et coûts financiers**	Un port peut perdre beaucoup d'argent en raison de l'arrêt des opérations ou du budget de réparation, en cas de dommages sur ses systèmes et infrastructures
	**Fraude et vol d'argent**	Comme toute grande entreprise, les systèmes financiers des ports peuvent être compromis pour leur voler de l'argent. En effet, en particulier pour les plus grands ports, les revenus portuaires sont importants : par exemple, les chiffres d'affaires de l'ensemble HAROPA (grands ports maritimes du HAVRE et de ROUEN et port autonome de PARIS) et du grand port maritime de MARSEILLE étaient respectivement en 2019 de 377,3 et 169,5 millions d'Euros. De plus, les ports étant la frontière entre deux États ou continents, les entreprises frauduleuses peuvent falsifier leurs déclarations en douane (fraude à la taxe sur la valeur ajoutée).
	**Dommages aux systèmes ou pire, destruction**	En raison de la grande complexité des systèmes et des infrastructures portuaires, dont certains sont critiques (par exemple, les systèmes industriels qui gèrent de grandes quantités de marchandises dangereuses), des dommages ou pire, la destruction de ces systèmes et infrastructures a des conséquences désastreuses pour le port opérations et sûreté et sécurité, y compris les personnes. Les pétroliers (en particulier les produits raffinés et le gaz) sont très vulnérables aux incendies et aux explosions ; le stockage local des produits inflammables et des produits chimiques est peut-être également massif.
	**Réputation ternie, perte de compétitivité**	Aujourd'hui, les ports sont dans un écosystème international extrêmement compétitif : le moindre incident ou problème sur ses activités et opérations peut nuire à sa réputation et perdre des clients qui pourraient diriger leur trafic vers les ports voisins.
	**Catastrophe environnementale**	Le port étant l'interface directe entre l'arrière-pays et la mer, une catastrophe environnementale dans les zones portuaires peut avoir des conséquences désastreuses sur les populations, la faune et la flore et les infrastructures humaines, à très longue distance (marée noire, explosion de gaz, pollution des océans), naufrages, etc.).

Enfin, les principales menaces auxquelles les écosystèmes portuaires peuvent être exposés sont décrites dans la figure 6 (source ENISA) et détaillées dans le tableau 4.

Figure 6 : Description détaillée des menaces (source ENISA)

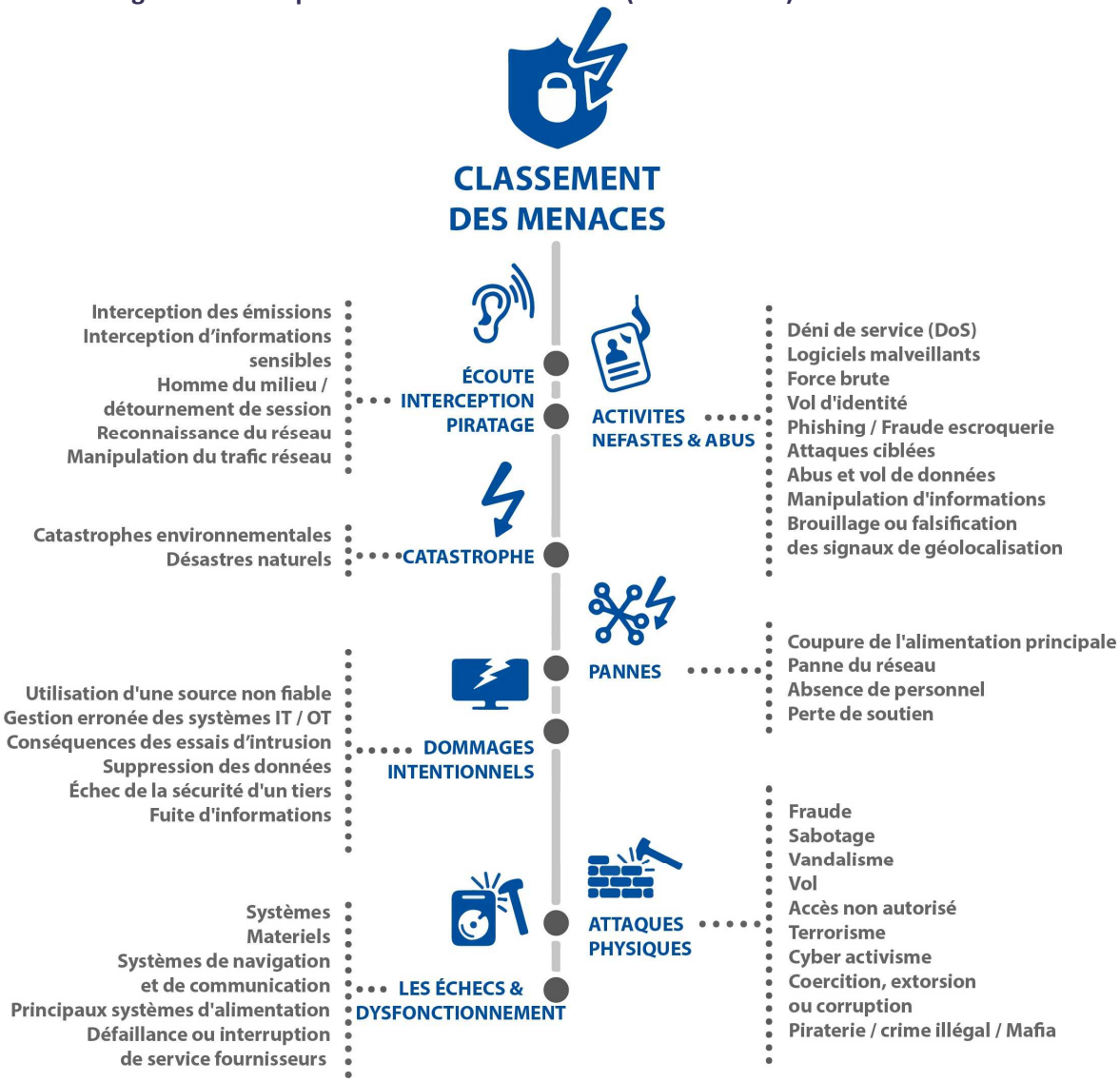


Tableau 4 : Description des menaces

Espionnage		
Mode opératoire (exemple)	**Sous-catégorie**	**Description & objectifs poursuivis**
Attaque de l'homme du milieu (« Man-in-the-middle ») & Interceptions	**Détournement de session**	Relayer et modifier éventuellement la communication entre deux parties qui croient qu'elles communiquent directement entre elles.
	Piratage d'une session	Exploiter les vulnérabilités des systèmes pour obtenir les mêmes droits d'accès que les clients ciblés (cookies d'authentification par exemple).
	Interception des émissions	Intercepter la communication entre le port et les différentes parties prenantes (radio, échanges entre navires et port, etc.).
	Interception de données sensibles	Ecouter les communications ou analyser les systèmes pour intercepter des données sensibles à des fins d'espionnage d'entreprise, d'espionnage d'État ou de criminalité et d'espionnage piraté.
Reconnaissance du réseau et manipulation du trafic	-	Scanner le réseau passivement jusqu'à trouver une porte d'entrée qui permette à l'attaquant de révéler des informations sur le réseau du port interne (ports ouverts, protocoles utilisés, etc.). Avec cette connaissance, l'attaquant opère pour comprendre les systèmes ciblés.
Attaque par point d'eau	**Défaillances et dysfonctionnements des systèmes des autres parties prenantes**	Exploiter les vulnérabilités - liées à des dysfonctionnements ou des défaillances - comme une porte d'entrée vers différents systèmes (navigation, communication et autres systèmes) d'autres acteurs portuaires (navires, autres acteurs du transport, etc.) liés à des systèmes portuaires.
Déstabilisation, atteinte à l'image ou neutralisation		
Mode opératoire (exemple)	**Sous-catégorie**	**Description & objectifs poursuivis**
Injection de code HTML, SQL, Javascript	**Défiguration**	Altérer l'apparence d'un site Internet et démontrer de la part de l'attaquant qu'il a pu prendre le contrôle du serveur, et donc, accéder potentiellement à des données sensibles (personnelles, bancaires, commerciales, etc.) : ce qui porte directement atteinte à l'image et à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires, etc.

Déni de service (DoS)	-	Cibler différents systèmes : RGPS, réseau, applications, IoT, etc… Les objectifs d'une telle attaque sont d'entraîner une indisponibilité du système et une interruption de la production. La plupart des attaques DoS sont causées par plusieurs sources en même temps (par exemple, un grand nombre de demandes envoyées par différents systèmes en même temps) envoyées au système cible, également appelé déni de service distribué (DDoS).
Force brute	-	Obtenir un accès non autorisé aux ressources d'une organisation (c'est-à-dire périphériques, etc.) à travers de nombreuses tentatives pour deviner la clé ou le mot de passe correct. Si les systèmes de port permettent l'utilisation de mots de passe simples ou par défaut, ils peuvent être particulièrement vulnérables à ce type d'attaques.

Cybercriminalité		
Mode opératoire (exemple)	**Sous-catégorie**	**Description & objectifs poursuivis**
Ingénierie sociale	-	Utiliser une interaction humaine pour obtenir ou compromettre des informations sur l'organisation et les processus portuaires : en posant des questions, en se faisant passer pour une autre personne, l'attaquant peut rassembler les informations dont il a besoin pour infiltrer les systèmes portuaires. L'attaquant peut demander plusieurs sources, en s'appuyant sur les informations qu'il peut obtenir de la première source pour ajouter à sa crédibilité ou en envoyant des liens malveillants.
	Hameçonnage (phishing)	Utiliser des mels ou des sites Web malveillants pour solliciter des informations personnelles en se faisant passer pour une organisation digne de confiance. Les attaques par phishing sont les attaques d'ingénierie sociale les plus courantes. D'autres formes existent : attaque par vishing (via la communication vocale), attaque par smishing (exploitation de SMS, texte, messages contenant un lien malveillant, etc.).
	Usurpation d'identité	Utiliser délibérément l'identité d'une personne impliquée dans l'écosystème portuaire, par exemple en volant des informations d'identification, pour obtenir un gain financier, des informations critiques, un accès non autorisé à un système, etc. La fraude du « faux président », en utilisant l'identité de personnes puissantes dans l'écosystème, peut avoir un impact sérieux.
Logiciels malveillants (Malware)	-	Faire pénétrer des logiciels malveillants dans les systèmes portuaires qui peut conduire à des actions indésirables et non autorisées, exploitant pour certaines d'entre elles des vulnérabilités pour élever les privilèges qui peuvent endommager les systèmes IT / OT du port, l'infrastructure, l'intégrité des données et les opérations. Il existe différents types de logiciels malveillants créés à des fins différentes : rançongiciels, virus, chevaux de Troie, logiciels espions, attaques par injection ou application Web, etc.

	Attaques ciblées	Cibler spécifiquement le port, de manière sophistiquée et malveillante, pour infiltrer ses systèmes à des fins différentes. Par exemple, la menace persistante avancée (APT) est une attaque furtive, diffuse et continue sur une longue période de temps conçue pour intégrer du code malveillant dans des systèmes ciblés qui effectuent des tâches spécifiques sans être remarqué.
	Abus et vol de données	Dérober, par différents moyens, des données sensibles (données personnelles, données de suivi de fret, données opérationnelles, etc.) et / ou abuser des certificats utilisés dans les opérations portuaires (certificats de navire, etc.).
	Manipulation des données	Manipuler des données (données financières, données de navigation, données de fret, opérations, etc.) dans les systèmes pour atteindre ses objectifs.
Signaux de géolocalisation usurpation / brouillage	-	Manipuler des systèmes de géolocalisation et de navigation pour modifier la trajectoire d'un navire, provoquer des accidents par exemple. Des attaques récentes utilisant l'usurpation GPS et la falsification AIS montrent que cette menace est importante et doit être prise en compte, en particulier dans le contexte maritime.

Tableau 4 bis : Autres menaces pouvant être prise en compte

Attaques physiques	
Sous-catégorie	**Description & objectifs poursuivis**
Accès non autorisé	Contourner les systèmes de contrôle d'accès pour pénétrer dans les zones portuaires, accéder à un navire ou à d'autres véhicules ou dispositifs terminaux OT (grues, etc.). De plus, des véhicules et des navires non autorisés peuvent également entrer dans les zones portuaires.
Fraude	Tromper intentionnellement la victime en violant le droit civil à différentes fins.
Extorsion	Chercher à obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque.
Corruption	Adopter un comportement malhonnête ou illégal visant des personnes puissantes dans un écosystème (par exemple dans l'écosystème portuaire) aux fins d'obtenir de leur part un quelconque avantage.
Hacktivisme	Utiliser la technologie pour promouvoir un programme politique ou un changement social.
Vol	Voler des appareils mobiles (téléphone portable, radios, etc.), du matériel fixe, des sauvegardes, des documents imprimés (liste des marchandises, navires, etc.), du fret (marchandises, fret, conteneur, etc.).
Vandalisme	Détériorer ou détruire volontairement des actifs portuaires sans raison particulière, tels que les systèmes informatiques et OT portuaires, les navires ou autres véhicules, et le fret (marchandises, fret, conteneur, etc.).
Sabotage	Détériorer ou détruire délibérément les systèmes et infrastructures portuaires afin d'affaiblir l'écosystème portuaire (principalement à des fins militaires, politiques ou idéologiques). Le sabotage peut être externe (de personnes qui ne sont pas directement impliquées dans les opérations portuaires) ou interne (de personnes directement impliquées dans les opérations portuaires, comme des employés irrités, etc.).
Terrorisme	Utiliser la violence intentionnelle, généralement contre des civils, à des fins politiques, idéologiques et religieuses
Piraterie, criminalité illégale, mafia	Développer des organisations illégales et non autorisées qui enfreignent la loi pour maintenir un pouvoir et des activités illégales (trafic de drogue, vol de marchandises, etc.).

Dommages involontaires	
Sous-catégorie	**Description & objectifs poursuivis**
Utilisation d'une source non fiable	L'utilisation d'une source non fiable pour les systèmes de port (mise à jour défectueuse, logiciel malveillant, etc.) peut entraîner un dysfonctionnement ou une propagation des systèmes. L'attaque NotPetya en est un parfait exemple.
Administration erronée des systèmes IT / OT	Même avec de bonnes intentions, si les administrateurs des systèmes portuaires ne sont pas suffisamment formés et informés des impacts de telles erreurs, une administration erronée peut avoir un impact important sur les systèmes portuaires et, si elles sont critiques, directement sur le port opérations.
Résultat des tests de pénétration	Afin de tester le niveau de sécurité des systèmes portuaires, le port peut ordonner des tests de pénétration qui, s'ils ne sont pas effectués correctement, pourraient endommager les systèmes.
Suppression de données	Par erreur, les employés ou autres parties prenantes accédant aux systèmes portuaires peuvent supprimer des informations critiques qui pourraient avoir un impact sur les opérations portuaires (par exemple, les informations de fret ou de navigation).
Défaillance de sécurité tierce	Les systèmes portuaires sont gérés et maintenus par différents prestataires de services : si leurs accès ne sont pas correctement contrôlés, les failles de sécurité de la tierce partie peuvent affecter directement les systèmes portuaires (en cas de maintenance par exemple).
Fuite d'informations	Les employés peuvent partager, par erreur ou par ignorance, des données sensibles si la solution de sensibilisation et de protection des données est insuffisante.

Défaillances et dysfonctionnements	
Sous-catégorie	**Description & objectifs poursuivis**
Défaillances ou dysfonctionnements des systèmes ou des dispositifs	Une défaillance ou un dysfonctionnement des systèmes informatiques ou OT ou des appareils terminaux peut parfois se produire, en particulier si la maintenance et la conformité aux manuels et instructions pendant l'exploitation ne sont pas assurées, ou si la bonne le fonctionnement n'est pas mesuré et contrôlé régulièrement.
Exploitation des vulnérabilités des systèmes ou des appareils	Les systèmes et les appareils peuvent présenter des vulnérabilités qui pourraient être exploitées par des pirates, en particulier si les systèmes ou les appareils ne sont pas corrigés à temps ou régulièrement surveillés alors que des mesures correctives sont mises en place entre-temps.
Défaillances et dysfonctionnements des systèmes des autres parties prenantes	Les systèmes (navigation, communication et autres systèmes) d'autres acteurs portuaires (navires, autres acteurs du transport, etc.) peuvent présenter des dysfonctionnements ou des défaillances pouvant entraîner un ralentissement voire un arrêt des opérations portuaires. De plus, si ces systèmes sont liés à des systèmes portuaires, un attaquant peut exploiter les vulnérabilités de ces systèmes comme une porte d'entrée vers des systèmes portuaires.
Principaux systèmes d'approvisionnement	Le port dépend de différents systèmes d'approvisionnement (électricité, carburant, etc.) qui sont essentiels pour assurer les opérations portuaires : en cas de panne ou d'interruption de ces systèmes, les opérations portuaires seront ralenties voire arrêtées.
Échec ou interruption des fournisseurs de services	Le port dépend de nombreux fournisseurs de services, et certains d'entre eux peuvent être critiques pour les opérations portuaires. Une défaillance ou une interruption de ces fournisseurs de services peut avoir un impact important sur les opérations portuaires.

Pannes	
Sous-catégorie	**Description & objectifs poursuivis**
Pannes principales d'alimentation	Les pannes sur l'alimentation principale peuvent avoir des impacts importants sur les opérations portuaires : l'arrêt de l'alimentation en carburant conduit à bloquer les navires dans le port, les pannes sur les réseaux électriques impactent les systèmes IT et OT (ex. : aucune communication possible entre les acteurs portuaires, le stockage frigorifique ne peut plus conserver les produits surgelés).
Panne de réseau	Les réseaux portuaires sont essentiels pour les opérations portuaires et la communication entre les différents acteurs (autorité portuaire, opérateurs de terminaux, navires, autres autorités, etc.) : les défaillances des réseaux portuaires peuvent affectent fortement leurs opérations.
Absence de personnel	Un incident peut se produire à un moment où les employés du port ne sont pas présents et peut avoir des conséquences importantes sur les systèmes et les infrastructures portuaires, en particulier dans le cas d'une automatisation croissante des processus portuaires.

3.2 Enjeux de cybersécurité

Les principaux enjeux auxquels les ports sont actuellement confrontés pour mettre en œuvre les mesures de cybersécurité sont les suivants :

- manque de culture numérique dans l'écosystème portuaire, dans lesquels certaines parties concernées sont encore conservatrices. En effet, de nouvelles tendances telles que la numérisation et les initiatives IoT entrent en collision avec la nature conservatrice de l'industrie maritime, mais sont de plus en plus appliquées. Dans ce contexte, les besoins de cybersécurité et les meilleures pratiques de ces initiatives ne sont souvent pas considérées comme prioritaires par les parties prenantes qui se penchent d'abord sur l'adoption des technologies ;

- manque de sensibilisation et de formation concernant la cybersécurité : l'écosystème des ports appréhende en premier lieu les enjeux de sécurité et de sûreté « physiques », alors que les systèmes d'information et de communication sous-tendent de nouveaux défis en matière de cybersécurité que les acteurs portuaires n'anticipent et ne maîtrisent souvent pas pleinement ;

- manque de temps et de budget alloué à la cybersécurité : en raison d'une mauvaise sensibilisation, en particulier de la direction en ce qui concerne les défis de la cybersécurité.

Complexité de l'écosystème portuaire du fait du nombre et de la diversité des acteurs impliqués dans les opérations portuaires : les acteurs au sein d'un port peuvent être nombreux (jusqu'à plusieurs centaines pour les plus grands ports).

Cet écosystème est construit à partir d'entreprises de différentes tailles, avec différents niveaux de capacités de cybersécurité.

Cela rend difficile le contrôle global de la cybersécurité au niveau du port avec un niveau hétérogène de contrôles au sein du port.

- Besoin de trouver un juste équilibre entre l'efficacité commerciale et la cybersécurité, notamment en garantissant la continuité des services tout en préservant la sécurité des TI et des OT, comme la déconnexion des systèmes critiques et la mise à jour des systèmes sans aucun impact commercial.

- Héritage de certains systèmes et pratiques : en particulier en ce qui concerne les systèmes de gestion des données de navigation et les systèmes OT qui peuvent être très anciens et vulnérables et pour lesquels des mesures de cybersécurité supplémentaires doivent être appliquées.

- Absence d'exigences réglementaires en matière de cybersécurité : la directive SRI / NSI est une première base pour mettre en œuvre des mesures de cybersécurité, mais ne concerne que certains des acteurs du secteur maritime. Cela n'est pas encore suffisant pour garantir un niveau de cybersécurité adéquat sur l'ensemble de l'écosystème portuaire et pour permettre le dégagement de budgets suffisants pour répondre aux exigences.

- Difficulté à se tenir au courant des dernières menaces, notamment au vu de la diversité des acteurs opérant dans les ports, des processus, des systèmes mis en place et utilisés et de la croissance rapide des innovations dans l'écosystème portuaire (solution proposée : s'abonner à la veille ANSSI).

- Complexité technique des systèmes informatiques et industriels du port : les parties prenantes du port utilisent différents systèmes qui sont développés, gérés et entretenus par différentes équipes ou entités. Par exemple, ils peuvent être développés soit par des équipes informatiques portuaires, soit par des tiers ou par des prestataires

informatiques. De plus, ils peuvent être basés sur différentes technologies. Enfin, les équipes gérant la sécurité des systèmes IT et OT peuvent également être différentes. Par conséquent, la cartographie de tous les systèmes portuaires est difficile à définir et à maintenir dans le temps.

- Convergence et interconnexion informatique et industriels : les systèmes industriels, généralement plus vulnérables que les systèmes informatiques, sont généralement protégés car ils sont séparés des systèmes et réseaux informatiques. Mais, de plus en plus, les systèmes et réseaux informatiques et industriels deviennent de plus en plus dépendants et interconnectés, exposant les systèmes industriels à des risques plus élevés.

- Défis de la chaîne d'approvisionnement. Un certain nombre de défis liés à la cybersécurité sont associés à la chaîne d'approvisionnement : manque de certifications de cybersécurité pour les produits et services portuaires, risques de sécurité liés à l'accès à distance des fournisseurs aux réseaux / systèmes portuaires, longs cycles de correction pour certains types de systèmes (par exemple ICS), hétérogénéité et nombre élevé de fournisseurs, difficulté de changer les services des fournisseurs. Les entrepreneurs n'ont pas beaucoup de contrôle sur le niveau de cybersécurité de leurs fournisseurs et, par conséquent, sur les cyberrisques qu'ils impliquent (attaques de la chaîne d'approvisionnement).

- Fortes interdépendances entre les systèmes et services portuaires et les services externes d'autres secteurs (par exemple l'énergie) qui introduisent des risques de cybersécurité d'interdépendance.

- Nouveaux cyber-risques résultant de la transformation numérique des ports : les ports lancent actuellement plusieurs projets de digitalisation des processus portuaires, notamment avec l'émergence du concept SmartPort, les cyber-risques devraient être pris en compte dans les phases initiales de ces projets.

3.3 Scénarios types de cyberattaques

Sur la base de la description des actifs et des menaces répertoriées dans les sections 2.1 et 3.1, plusieurs scénarios types de cyberattaques ont été définis en corrélation avec les sources de menaces et les possibles impacts sur les actifs portuaires, énumérés et détaillés dans la section 3.1. Chaque scénario est associé à une liste de mesures de sécurité, détaillée plus loin dans le chapitre 4, qui atténuera le risque que ce scénario se produise. Les mesures de sécurité sont formalisées sous la forme, pour prendre un exemple, de « TP-01 : segmentation du réseau », avec « TP » comme groupe de mesures (dans ce cas « Pratiques techniques »), le numéro associé (dans ce cas « 01 ») et le nom de la mesure (dans ce cas « Segmentation du réseau »).

Scénario A - Compromission de données critiques pour voler des marchandises de grande valeur ou autoriser le trafic illégal par le biais d'une attaque ciblée

Ce scénario est une attaque sophistiquée et ciblée contre les systèmes portuaires (menace persistante avancée) : les attaquants doivent avoir une connaissance approfondie des systèmes et réseaux portuaires (ingénierie sociale, analyse du réseau), des processus portuaires et de l'infrastructure portuaire (intrusion physique) pour effectuer des cargaisons et vol de conteneurs. Un exemple d'une telle attaque s'est produite dans l'un des terminaux portuaires d'Anvers en Belgique.

Impacts		
Vols de marchandises	Trafics illégaux	Réputation ternie

Actifs touchés	Acteurs impliqués
Systèmes communautaires de fret (CCS) Réseaux Courriel Personnes	Opérateurs de terminaux Police Compagnies de transport maritime et de fret maritime Expéditeurs et destinataires

Détails de l'attaque

D'une part, les attaquants identifient et récupèrent les données d'authentification (informations d'identification) pour accéder à des systèmes utiles :

- les attaquants rassemblent des informations sur les systèmes portuaires par le biais de l'ingénierie sociale ;
- ensuite, ils identifient les systèmes ciblés utilisés pour la gestion des cargaisons et des conteneurs et l'identité des personnes qui les utilisent ;
- une fois les systèmes et leurs opérateurs / utilisateurs identifiés, les attaquants lancent des attaques de phishing pour récupérer les informations d'identification pour accéder à ces systèmes.

D'autre part, les attaquants installent des composants pour accéder à distance au réseau portuaire et contourner la sécurité du réseau :

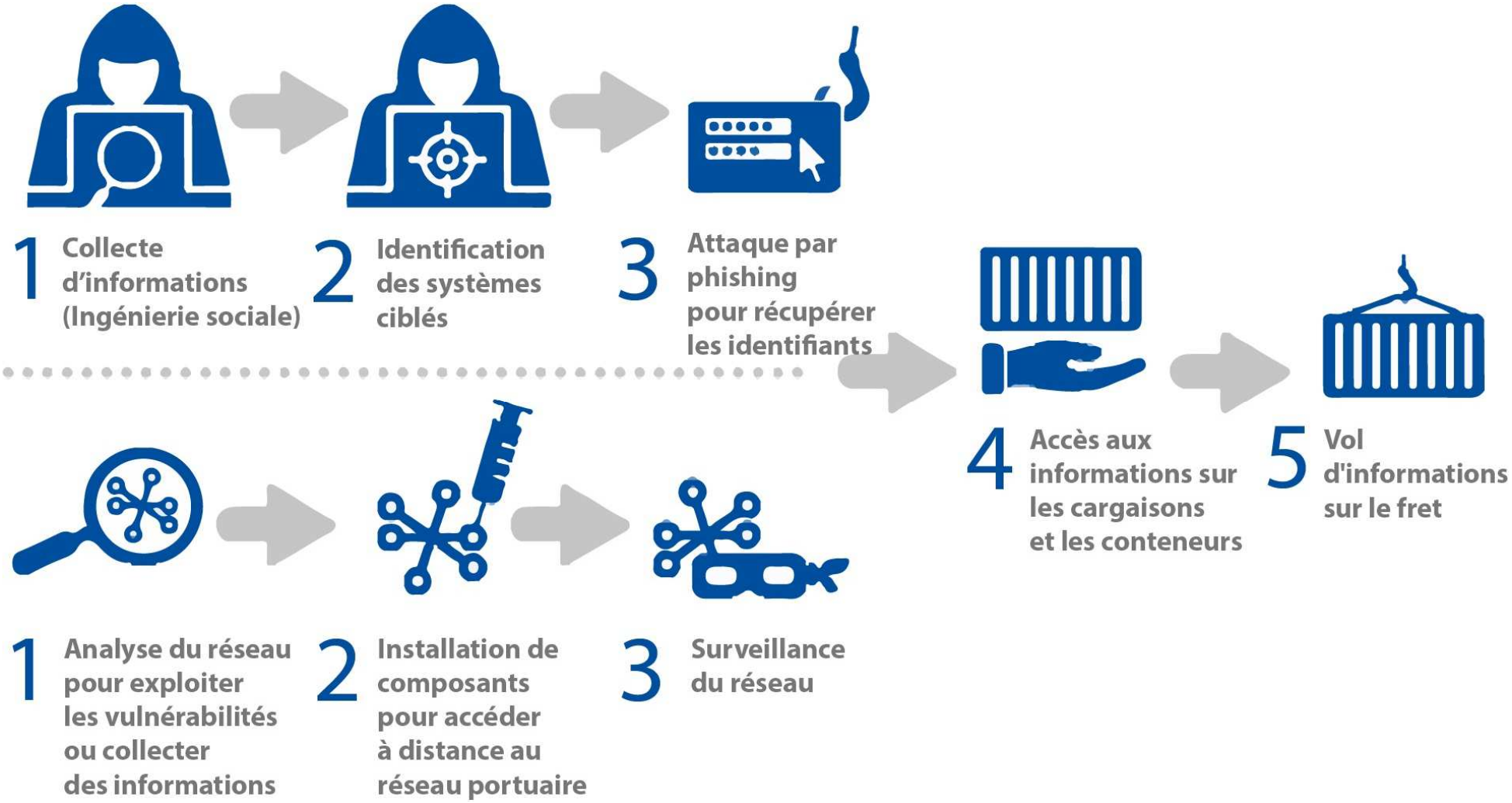
- les attaquants scannent les réseaux portuaires pour trouver des vulnérabilités afin de les exploiter et recueillir des informations ;
- ils installent, si nécessaire, par intrusion physique, des composants pour accéder à distance aux réseaux portuaires (point d'accès sans fil) ;
- pour assurer un accès constant et s'adapter à chaque réseau et infrastructure changements à long terme, ils espionnent les réseaux.

Les attaquants ont désormais accès au suivi du fret systèmes et autres systèmes portuaires pertinents et ils peuvent accéder aux informations critiques sur les conteneurs qu'ils veulent voler (localisation, contenu, code de ramassage, etc.) de l'extérieur des installations portuaires.

Les attaquants peuvent alors voler la cargaison avant la date de retrait officielle.

Principales mesures de cybersécurité	
OP-10 : programme de sensibilisation à la sécurité.	**TP-01 : segmentation du réseau.**
OP-16 : création d'un centre d'opérations de cybersécurité (SOC).	**TP-02 : analyses régulières du réseau.**
	TP-08 : authentification multifacteur.

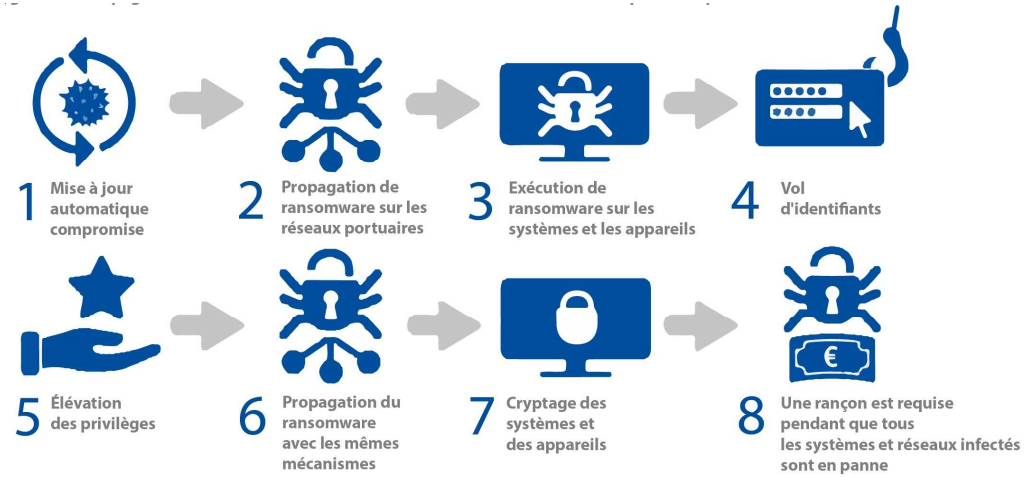
Figure 7 : Compromission de données critiques pour voler des marchandises de grande valeur ou autoriser un scénario de trafic illégal (source ENISA)



Scénario B - Propagation d'un ransomware entraînant un arrêt total des opérations portuaires

Ce scénario peut être une attaque ciblée ou non ciblée (comme dommages collatéraux d'une attaque ciblée sur d'autres sociétés par la propagation du rançongiciel) : les pirates peuvent développer un rançongiciel exploitant différentes vulnérabilités pour le diffuser dans les réseaux portuaires et chiffrer les différents systèmes périphériques (postes de travail, serveurs, etc.), entraînant la destruction des systèmes infectés et la perte potentielle de sauvegardes (au sein de serveurs pouvant être chiffrés). Un exemple d'attaque malveillante destructrice de type ransomware a été l'incident à grande échelle affectant les opérations de Maersk.

Figure 8 : Propagation de ransomware conduisant à un arrêt total des opérations portuaires (source ENISA)



Impacts		
Réputation ternie	Perte et coûts financiers	Dommages aux systèmes ou, pire, destruction

Actifs touchés	Acteurs impliqués
Arrêt des opérations portuaires, paralysie portuaire Actifs concernés Parties prenantes impliquées Systèmes informatiques Systèmes et réseaux OT Terminaux OT Personnes Informations et données	Tous acteurs du port

Détails de l'attaque

Le port met à jour l'un de ses serveurs avec une mise à jour compromise (ransomware) - d'autres moyens peuvent être utilisés pour introduire un ransomware sur les systèmes portuaires, par exemple l'ingénierie sociale (phishing ou USB-drop par exemple) ou une mauvaise ségrégation du réseau (large exposition à Internet).

Le ransomware se propage dans le réseau du port, en utilisant des vulnérabilités non corrigées et un manque de segmentation du réseau. Il est exécuté sur les systèmes et appareils du port et dérobe les informations d'identification stockées. Il exécute un mécanisme d'élévation des privilèges, en utilisant une mauvaise séparation des comptes hautement privilégiés. Il se propage dans d'autres parties du réseau du port par le même mécanisme. Il infecte les systèmes et les appareils cryptés ne peuvent plus être utilisés.

Une rançon est requise alors que tous les systèmes et appareils sont en panne.

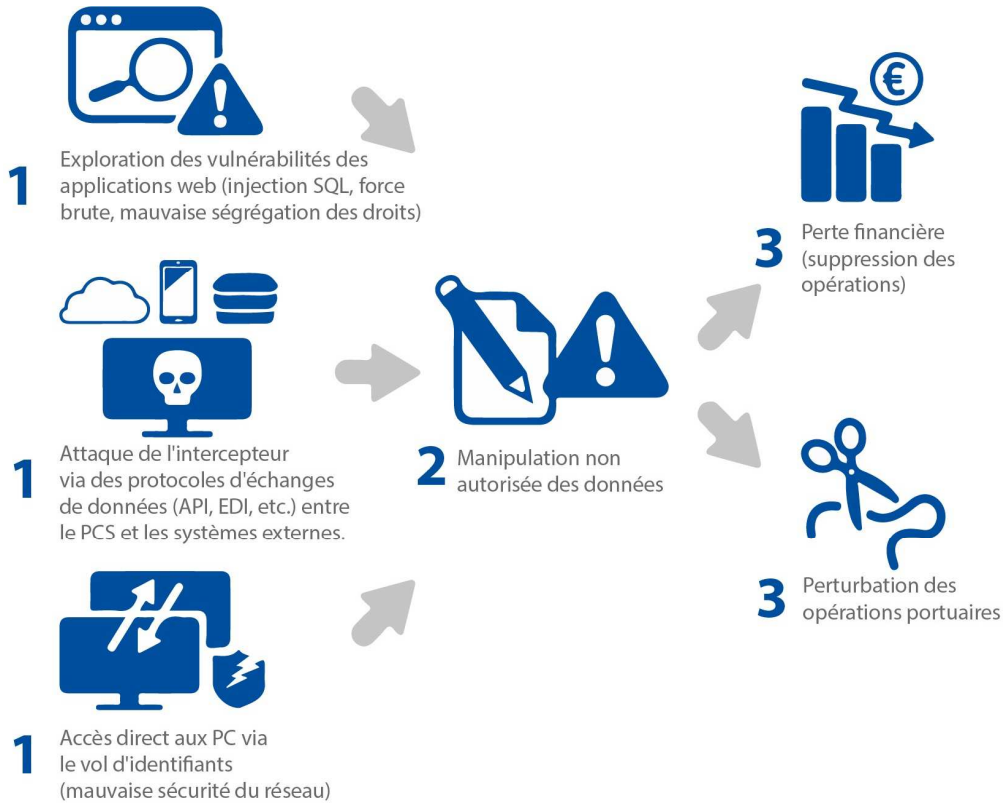
Principales mesures de cybersécurité	
OP-01 : Stratégie de protection des points d'extrémité.	**TP-01 : Segmentation du réseau**
OP-05 : Définir un processus de gestion des vulnérabilités.	**TP-13 : Gestion des comptes privilèges (« PAM »).**
OP-16 : Création d'un centre d'opérations de cybersécurité (SOC).	**TP-15 : Gestion anti-malware et anti-virus.**
	TP-23 : Processus de gestion des mises à jour.
PS-15 : Assurer la cyber résilience du port systèmes.	**TP-24 : Source de vérification des mises à jour.**
PS-17 : définir une organisation de gestion de crise.	

Scénario C - Compromission du système de communauté portuaire pour manipulation ou vol de données

Ce scénario est une attaque ciblée contre les systèmes utilisés pour les échanges entre toutes les parties prenantes (généralement les systèmes communautaires portuaires). Les objectifs sont de falsifier les informations sur les services portuaires pour perturber les opérations ou modifier certaines opérations dans les systèmes (impliquant une perte financière pour le port). Ce scénario est réaliste car ces systèmes sont exposés à toutes les parties prenantes du port de différentes manières (généralement en utilisant différents réseaux et systèmes, via un accès VPN ou via Internet, la plupart du temps via des interconnexions de machine à machine). En effet, ces systèmes sont de plus en plus automatiquement interconnectés avec des systèmes externes (via API, échanges EDI, etc.) : les systèmes de tiers deviennent ainsi une surface d'attaque supplémentaire pour atteindre les systèmes portuaires.

Étant donné que ces systèmes sont différents d'un port à l'autre, il peut y avoir plusieurs façons de configurer cette attaque: par exemple, si les systèmes de communauté de port sont exposés via une application Web, l'attaquant peut exploiter les vulnérabilités courantes des applications Web ; s'il s'agit d'une application développée en interne par des développeurs employés par le port et si des règles de développement de sécurité standard ne sont pas appliquées, des vulnérabilités spécifiques peuvent être exploitées, etc.

Figure 9 : Compromission du système de la communauté portuaire pour la manipulation ou le vol de scénario de données (source ENISA)



Impacts		
Perte financière	Perturbation des opérations portuaires	Accident (lié à la gestion des marchandises dangereuses)

Actifs touchés	Acteurs impliqués
Systèmes communautaires portuaires (PCS) Systèmes financiers · ERP	Autorité portuaire Opérateurs de terminaux portuaires

Détails de l'attaque

Selon l'architecture du PCS et l'exposition du réseau: o Si le PCS est exposé à des tiers via une interface Web dédiée, l'attaquant peut exploiter les vulnérabilités courantes des applications Web pour avoir accès au PCS (injection SQL « langage de requête structuré », attaque par force brute, exploitation de mauvaise ségrégation des droits d'accès, etc.).

- Si le PCS est automatiquement connecté à des systèmes externes via des protocoles d'échange de données tels que des protocoles API ou EDI, l'attaquant peut organiser une attaque de type intermédiaire en interceptant les échanges de données et en les modifiant dans le cas où les échanges de données ne sont pas suffisamment sécurisés.

- Si un accès direct au PCS lui-même hors du réseau portuaire est possible, l'attaquant peut exploiter des mesures de sécurité de réseau faibles pour avoir un accès direct à ce système et utiliser des informations d'identification qu'il a pu avoir volées via l'ingénierie sociale.

Une fois que l'attaquant a un accès non autorisé au PCS avec suffisamment de droits d'accès, il peut manipuler les données directement sur le PCS (modification des opérations portuaires, vol de données critiques, suppression de données sur certaines opérations, etc.).

La perte de l'intégrité des données PCS a de nombreuses conséquences: chaos dans les opérations portuaires, perte financière potentielle pour le port qui perd des informations sur les opérations l'empêchant de facturer les opérations effectuées ou même accident si des marchandises dangereuses liées aux données sont manipulées ou rendues indisponibles

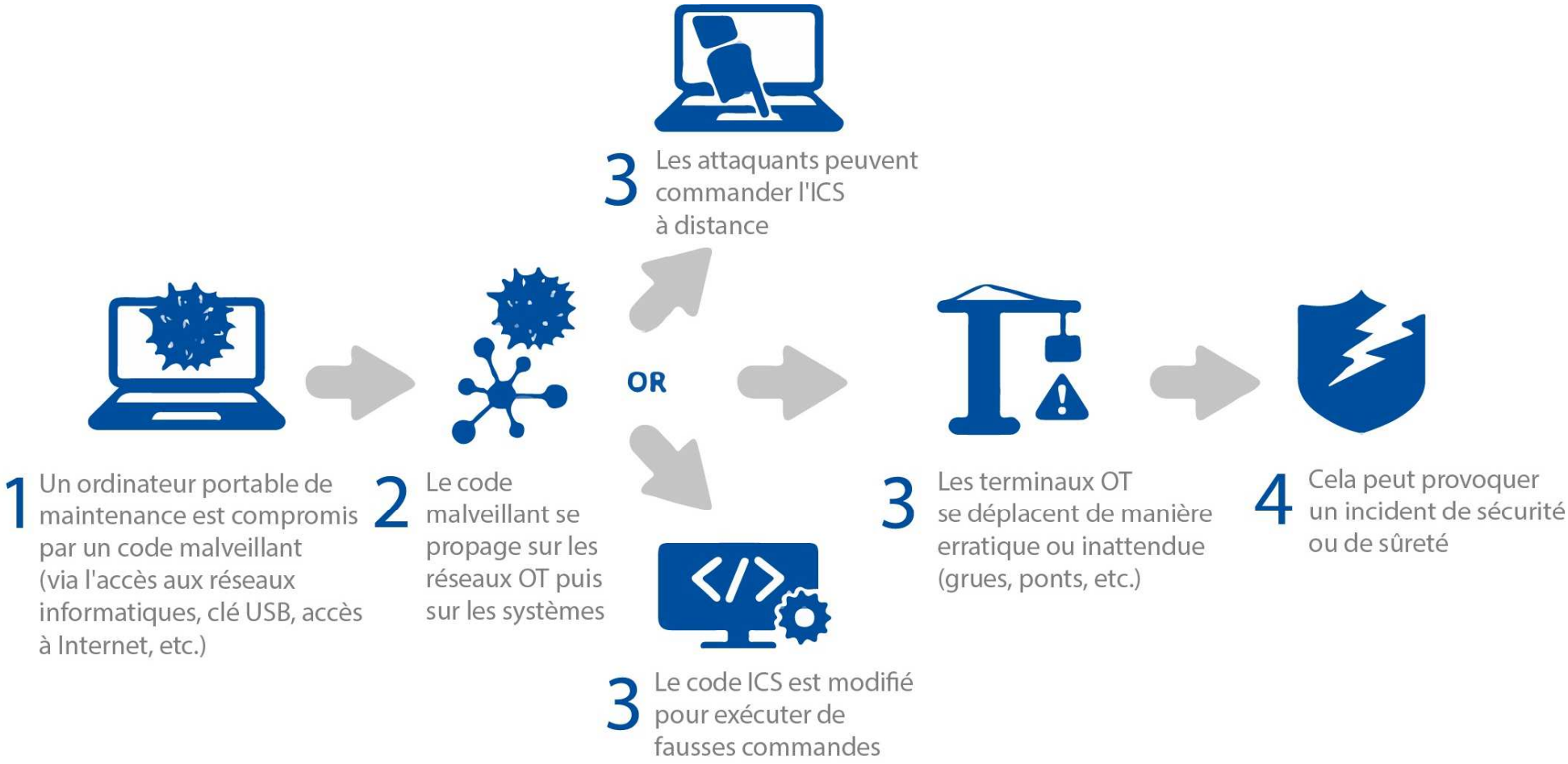
Principales mesures de cybersécurité	
PS-09 : méthodologie du projet, y compris les évaluations de sécurité et les points de contrôle.	**TP-01 : segmentation du réseau.**
	TP-05 : stratégie de gestion des identités et des accès (« IAM »).
	TP-08 : authentification multifacteur.
OP-11 : contrôle strict des accès des tiers.	**TP-19 : mécanismes sécurisés pour les échanges de machine à machine.**
OP-16 : création d'un centre d'opérations de cybersécurité (SOC).	**TP-25 : systèmes de corrélation et d'analyse des journaux.**
OP-17 : analyses régulières du réseau.	
OP-18 : sécurité du périmètre avec politique de filtrage.	
OP-19 : effectuer des audits de cybersécurité réguliers.	

Scénario D - Compromission de systèmes industriels créant un accident majeur dans les zones portuaires

Ce scénario est spécifique au monde OT et aux spécificités ICS et est considéré comme réaliste même si aucune attaque de ce type dans les ports n'est connue du public. En effet, des attaques similaires se produisent dans d'autres secteurs critiques, en particulier dans le secteur de l'énergie. Ce type d'attaque n'a pas besoin d'être généralement sophistiqué pour avoir un impact et les principaux risques restent la connexion avec les réseaux et systèmes externes, en particulier Internet. Les spécificités de ces attaques sont le lien étroit entre le monde physique et logique: l'attaque commence généralement dans le monde logique (à partir de la composante informatique) et a des impacts dans le monde physique (dommages aux systèmes industriels et aux appareils finaux, sûreté et sécurité, incidents, etc.).

Un port contient différents réseaux, systèmes et dispositifs terminaux industriels utilisés pour différents services et opérations et détenus, gérés et entretenus par différentes parties prenantes: grues pour le chargement et le déchargement des navires dans les terminaux portuaires, ponts à l'entrée du port pour y faire entrer les navires, les systèmes dans les entrepôts réfrigérés pour garder les aliments fragiles à une température sûre, les capteurs et les systèmes utilisés pour transporter, stocker et surveiller les marchandises dangereuses, etc.

Figure 10 : Compromission du système OT créant un accident majeur dans le scénario des zones portuaires (source ENISA)



Impacts		
Arrêt des opérations portuaires, paralysie portuaire	Dommages aux systèmes, ou pire, destruction	Blessures ou décès humains
Pertes et coûts financiers	Réputation ternie et perte de compétitivité	Catastrophe environnementale

Actifs touchés	Acteurs impliqués
Systèmes et réseaux OT Fin OT appareils Infrastructure mobile Infrastructure fixe Personnes	Autorité portuaire Opérateurs de terminaux portuaires Fournisseurs de services Chaîne de livraison

Détails de l'attaque

Un ordinateur portable de maintenance accédant aux systèmes de contrôle OT est compromis avec un code malveillant (via une clé USB ou un courrier électronique compromis, téléchargement de logiciels malveillants à partir d'Internet, etc.).

Le code malveillant se propage sur les réseaux OT, puis l'OT systèmes lorsque l'ordinateur portable s'y connecte.

Si les systèmes de contrôle industriel (ICS) sont sophistiqués (IoT, serveur distant, etc.), les attaquants peuvent déployer des mécanismes pour commander l'ICS à distance.

Sinon, le code ICS est modifié pour exécuter des commandes prédéfinies contenues dans le code malveillant.

Les dispositifs terminaux OT, tels que les grues ou les ponts, se déplacent de manière irrégulière ou inattendue.

Cela peut provoquer un incident de sécurité et de sûreté entraînant des dommages ou la destruction de l'infrastructure portuaire, des blessures ou la mort, etc.

Principales mesures de cybersécurité	
OP-01 : définir une stratégie de protection des points finaux.	**TP-11 : politique d'installation et de configuration.**
OP-09 : développer des cours de formation spécifiques et obligatoires sur la cybersécurité pour certaines populations clés.	**TP-14 : réseau d'administration dédié.**
OP-12 : définir clairement tous les aspects pertinents du partenariat avec des tiers, inclure des mesures de sécurité.	**TP-25 : systèmes de corrélation et d'analyse des journaux.**
OP -16 : créer un centre d'opérations de cybersécurité	**TP-30 : segmentation du réseau entre l'informatique et Systèmes OT.**
OP-21 et OP-22 : protéger physiquement les systèmes informatiques et OT.	**TP-29 et TP-31 : prise en compte des systèmes OT et IoT dans toutes les mesures de sécurité et mettre en place des mesures de sécurité spécifiques.**

3.4 Analyse du niveau de maîtrise – « Méthode EBIOS »

EBIOS Risk Manager (EBIOS RM) est la méthode d'appréciation et de traitement des risques numériques publiée par l'ANSSI avec le soutien du Club EBIOS.

Elle propose une boite à outils adaptable, dont l'utilisation varie selon l'objectif du projet et est compatible avec les référentiels normatifs en vigueur, en matière de gestion des risques comme en matière de sécurité du numérique. EBIOS RM permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maîtriser. Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue.

Enfin, cette méthode permet de faire émerger les ressources et arguments utiles à la communication et à la prise de décision au sein de l'organisation et vis-à-vis de ses partenaires.

Vous trouverez toutes les informations utiles à l'adresse suivante :
EBIOS Risk Manager

4. IDENTIFIER LES MESURES DE CYBERSÉCURITÉ ADAPTÉES

L'élaboration de mesures de cybersécurité pour les ports constitue l'un des points centraux de ce guide. L'objectif est de fournir des lignes directrices et des recommandations aux acteurs de l'écosystème portuaire pour les aider à prévenir, notamment via la réalisation d'auto-diagnostics, ou à répondre correctement aux cyberattaques potentielles sur les systèmes portuaires.

Pour définir la catégorisation de ces mesures, le guide s'est appuyé sur les scénarios types de cyberattaque identifiés dans la partie 3.3 ainsi que sur les mesures de sécurité des politiques et normes énumérées à la section 1.1 et les cadres communs pour la cybersécurité comme le Document de référence sur les mesures de sécurité pour les opérateurs de services essentiels, ISO 27001 ou NIST.

Enfin, une liste de 22 domaines de sécurité a été définie pour classer toutes les mesures de sécurité en relation avec les ports. Pour organiser les domaines de manière logique, ils ont été classés en trois groupes principaux :

- politiques et gouvernance
- pratiques et processus organisationnels
- pratiques et mesures techniques

Il existe 42 règles d'hygiène de l'ANSSI qui constituent une liste de règles les plus simples et les plus élémentaires mais essentielles pour assurer la sécurité de tout système d'information.

Elles sont à mettre en parallèle avec les 23 règles de sécurité imposées aux systèmes d'information essentiels des opérateurs de services essentiels sont d'un niveau d'exigence nettement plus élevé.

Étant donné qu'une partie du public cible de ce guide est éligible aux dispositions de la directive SRI / NIS en tant qu'opérateurs de services essentiels, les mesures suivantes ont été élaborées pour correspondre aux mesures proposées dans le document de référence sur les mesures de sécurité pour les opérateurs de services essentiels.

Néanmoins, quelques exceptions existent, notamment la sécurité du cloud, la sécurité machine à machine et la sécurité des systèmes de contrôle OT et industriels, ce qui indique qu'une approche plus sectorielle peut être pertinente pour répondre aux spécificités du secteur portuaire

Le code couleur utilisé ci-après est donc proposé à titre indicatif pour aider le lecteur à se situer entre ces deux niveaux d'exigence.

VERT : mesure ayant correspondance parmi les 42 règles du guide d'hygiène informatique de l'ANSSI et parmi les 23 règles du texte de transposition de la Directive NIS.

ORANGE : mesure non formulée de manière explicite dans les 42 règles guide d'hygiène informatique de l'ANSSI, mais parmi les 23 règles du texte de transposition de la Directive NIS.

BLEU : mesure ayant correspondance parmi les 42 règles guide d'hygiène informatique de l'ANSSI mais non parmi les 23 règles du texte de transposition de la Directive NIS.

ROUGE : mesure non formulée de manière explicite dans les 42 règles du guide d'hygiène informatique de l'ANSSI ni parmi les 23 règles du texte de transposition de la Directive NIS.

4.1 Politiques et gouvernance

Il est essentiel que les ports définissent les politiques et la gouvernance en matière d'IT et d'OT, en appliquant les meilleures pratiques de cybersécurité, en particulier pour la plupart des actifs critiques, avec une approche basée sur les risques.

4.1.1 Politique et organisation de la sécurité

Mesures de cybersécurité pour mettre en œuvre et maintenir à jour une politique de sécurité du système d'information (PSSI).

PS 01 Rédiger et mettre en œuvre une politique de sécurité des systèmes d'information (ISSP) qui décrit tous les moyens et procédures organisationnels et techniques, y compris les sujets liés à l'environnement OT. Cet ISSP doit être approuvé par la haute direction du port afin de garantir l'approbation de haut niveau de la politique. Les éléments clés de l'ISSP peuvent être intégrés dans le plan de sûreté de l'installation portuaire requis par le code ISPS.

PS 02 Appliquer la gouvernance de la sécurité des environnements IT et OT via l'ISSP en décrivant les rôles et les responsabilités de chaque partie prenante (exploitant, opérateurs de terminaux, prestataires, etc.).

PS 03 Partager cet ISSP avec toutes les parties prenantes impliquées dans les opérations portuaires ou, si plus pertinent, une version allégée sous-tendant les responsabilités de chaque partie envers la cybersécurité au niveau du port.

PS 04 Examiner annuellement la PSSI en tenant compte des résultats des tests de cybersécurité et de l'analyse des risques pour lutter contre les nouvelles menaces et les nouveaux risques

4.1.2 Gestion des risques et des menaces

Mesures de cybersécurité pour identifier et gérer en permanence les risques et menaces liés à l'écosystème portuaire.

PS 05 Adopter une approche fondée sur les risques pour élaborer la stratégie de cybersécurité des ports et mettre en place un processus d'amélioration continue pour s'assurer que les risques identifiés sont maîtrisés et que les nouveaux risques sont correctement identifiés en temps opportun. Veiller à ce que les cyber-risques identifiés soient pris en compte dans les plans de sûreté et de sécurité pour aligner la cybersécurité sur la sécurité et la sûreté physique (en particulier, grâce à l'évaluation de sûreté des installations portuaires requise par le code ISPS).

PS 06 Effectuer et mettre à jour régulièrement l'analyse des risques pour identifier les risques et les menaces liés à l'écosystème portuaire. En particulier, une analyse des risques doit être menée pour les nouveaux projets (initiatives SmartPort telles que Big Data, IoT, blockchain, etc.).

PS 07 Mettre en place des indicateurs de sécurité et des méthodes d'évaluation pour évaluer la conformité des systèmes et processus portuaires à l'ISSP et la performance de la gestion des risques, en impliquant plusieurs parties prenantes le cas échéant.

PS 08 Mettre en place un processus de renseignement sur les menaces pour surveiller en permanence les vulnérabilités, identifier les nouveaux risques et menaces et déployer des actions pour les atténuer.

Cette mesure peut être améliorée en développant des initiatives collaboratives privées-publiques de partage d'informations sur les renseignements sur les menaces au niveau européen.

4.1.3 Sécurité et confidentialité dès la conception

Mesures de cybersécurité qui doivent être appliquées dès les premières étapes du développement des systèmes et pendant le cycle de vie du développement afin d'augmenter par conception les niveaux de sécurité de toutes les solutions et applications, pour protéger les données critiques et garantir la confidentialité des données personnelles.

PS 09 Développer une méthodologie de projet comprenant des évaluations et des points de contrôle de sécurité, y compris pour les projets agiles (analyse des risques, examen de la sécurité de l'architecture, tests de sécurité, approbation de la sécurité, etc.) pour les projets nouveaux et existants, compte tenu de la criticité et de l'exposition du système. Plus précisément, inclure fortement les problèmes de cybersécurité dans les projets SmartPort, de la conception à la mise en œuvre.

PS 10 Résoudre les problèmes liés à la confidentialité sur la base des réglementations locales et internationales applicables, telles que le règlement général sur la protection des données (RGPD).

PS 11 Lancer un projet de classification des données pour identifier les données critiques pour les opérations portuaires ainsi que les données personnelles et pour les protéger en conséquence et pour cartographier les flux de données, en particulier pour les données personnelles et les données opérationnelles relatives aux navires, aux marchandises dangereuses et au fret.

4.1.4 Inventaire et gestion des actifs

Mesures de cybersécurité concernant la cartographie des écosystèmes, y compris les actifs des ports et les actifs de tiers interagissant avec les actifs du port.

PS 12 Utiliser des outils centralisés pour l'inventaire et la gestion des actifs et assurez-vous de les maintenir à jour (applications, plates-formes logicielles, réseaux, composants réseau, serveurs, périphériques physiques, systèmes industriels, composants d'administration, etc.).

PS 13 Définir une politique concernant les périphériques et logiciels autorisés pour garantir que seuls des composants fiables sont introduits dans le réseau de ports.

PS 14 Utiliser des outils centralisés pour surveiller les différents actifs en les adaptant en fonction des spécificités et des risques associés (par exemple surveillance passive pour les systèmes industriels) et détecter les actifs non autorisés.

4.1.5 Cyber-résilience

Mesures de cybersécurité mises en place pour assurer, en cas d'incident, ou pire, de catastrophe, la continuité des opérations portuaires et récupérer les données.

PS 15 Assurer la cyber-résilience des systèmes portuaires en définissant des objectifs et des directives stratégiques concernant la continuité des activités et la gestion de la récupération et mettre en place les services et processus clés associés (plan de continuité de l'activité / plan de reprise de l'activité ; en anglais, « Disaster Recovery Plan »).

PS 16 Définir des paramètres importants pour la continuité des activités du port, tels qu'un objectif de temps de récupération (« RTO »), un objectif de point de récupération (« RPO »), une interruption maximale tolérable (« MTO ») et un objectif de continuité des activités minimales (« MBCO »).

PS 17 Définir une organisation de gestion de crise en formalisant une politique spécifique et en mettant en place le processus de gestion de crise associé, incluant toutes les parties prenantes du port.

PS 18 Assurer l'efficacité des procédures de récupération en organisant des exercices de formation annuels, en s'assurant que toutes les parties prenantes critiques du port (autorités locales, autorités portuaires, opérateurs de terminaux, prestataires de services, etc.) sont impliquées autant que possible et formaliser les rapports post-exercice.

4.2 Pratiques et processus organisationnels

Les ports doivent définir les pratiques et processus pertinents concernant la gestion informatique et OT, à suivre par tous les employés du port ou plus spécifiquement par les équipes IT et OT dans leurs opérations quotidiennes au sein de l'écosystème portuaire.

4.2.1 Protection des terminaux et gestion du cycle de vie

Mesures de cybersécurité liées à la protection des terminaux informatiques tels que les ordinateurs portables, les ordinateurs de bureau, les tablettes, les téléphones portables.

OP 01 Définir une stratégie de protection des terminaux pour surveiller les terminaux des ports et renforcer leur sécurité en mettant en œuvre des outils et des mécanismes de sécurité tels que l'antivirus, le cryptage, la gestion des terminaux mobiles (« MDM ») et le renforcement (désactivation des services inutiles, notamment en sécurisant Ports USB dans tous les systèmes de ports).

OP 02 Implémenter des listes blanches d'appareils et de logiciels et révisez la liste au moins une fois par an ou en cas de changement majeur du système.

OP 03 Définir un processus de gestion du changement pour introduire tout nouveau dispositif dans les systèmes portuaires (tests d'acceptation, étapes de validation, etc.).

OP 04 S'assurer que tous les employés et sous-traitants retournent leurs terminaux à la fin du contrat et définir les processus d'élimination sécurisée des terminaux.

4.2.2 Gestion des vulnérabilités

Mesures de cybersécurité pour garantir que les systèmes sont à jour et protégés contre les vulnérabilités.

OP 05 Définir un processus de gestion des vulnérabilités pour identifier les vulnérabilités des actifs, il peut être basé sur des outils automatiques et manuels tels que les analyses de vulnérabilité.

OP 06 Définir des processus de renseignement pour la cybersécurité afin d'être au courant des vulnérabilités nouvellement révélées et de prendre des mesures compensatoires rapides (séparation du réseau, désactivation des services, etc.).

OP 07 Etablir une collaboration étroite entre les départements OT et IT, en veillant à ce que leur collaboration avec les propriétaires de systèmes, les autorités décisionnelles et les autres parties prenantes soit efficace et garantisse un niveau de cybersécurité homogène pour l'IT et l'OT.

4.2.3 Sécurité des ressources humaines

Mesures de cybersécurité pour assurer une bonne maîtrise des opérations IT et OT et une sensibilisation de tous les collaborateurs.

OP 08 Assurer des références professionnelles et des audits des casiers judiciaires du personnel clé pour la gestion informatique et OT (administrateurs système, développeurs, etc.) et du personnel clé nommé dans des rôles de sécurité (DSI ou DPO).

OP 09 Développer des cours de formation spécifiques et obligatoires sur la cybersécurité pour certaines populations clés traitant quotidiennement avec les IT et OT (administrateurs système, chefs de projet, développeurs, agents de sécurité, maître de port, etc.).

OP 10 Mettre en place un programme de sensibilisation à la sécurité pour adresser l'ensemble de l'écosystème portuaire, en se concentrant d'abord sur les principales menaces (par exemple l'ingénierie sociale).

4.2.4 Gestion de la chaîne d'approvisionnement

Mesures de cybersécurité pour comprendre et sécuriser la relation avec des tiers et garantir un accès légitime aux systèmes portuaires.

OP 11 N'accorder l'accès qu'à la demande, dans une fenêtre de temps spécifiée, dans un but spécifique et de la manière la moins privilégiée.

OP 12 Définir clairement tous les aspects pertinents du partenariat avec des tiers, y compris la sécurité, dans les accords et contrats appropriés, en particulier pour les systèmes critiques fournis par des tiers (PCS, CCS, systèmes de sécurité, etc.).

4.2.5 Détection et réponse aux incidents

Mesures de cybersécurité pour définir les processus de détection et de réponse aux incidents de sécurité survenant dans l'écosystème portuaire.

OP 13 Identifier les risques et menaces à tous les niveaux du port pour définir les catégories d'incidents et les impacts potentiels en utilisant les résultats de l'analyse des risques, du renseignement sur les menaces, de l'historique des incidents précédents, des discussions avec d'autres ports, etc.

OP 14 Définir une politique et des procédures pour la détection et la réaction aux incidents, y compris la description des rôles et responsabilités de chaque partie prenante au niveau du port ou de l'État (le cas échéant), ainsi que la méthode de coordination et la communiquer à toutes les parties concernées.

OP 15 Améliorer et maintenir ces procédures à jour en les testant grâce à des exercices de formation et en identifiant les nouveaux événements redoutés.

OP 16 Envisager la mise en place d'un centre d'opérations de cybersécurité (SOC) comprenant des environnements informatiques et OT pour prendre en charge la sécurité et les cyberincidents. Les SOC des différentes parties prenantes doivent collaborer (ou peuvent être mutualisés) pour assurer la détection et la réaction des incidents au niveau du port.

OP 17 Définir les procédures d'alerte et identifier les bons contacts pour chaque partie prenante du port en fonction de la criticité de l'incident (RSSI, direction et conseil d'administration du port, autorités nationales, équipe de réponse aux incidents de sécurité informatique « CSIRT », etc.).

OP 18 Mettre en œuvre des procédures de notification des incidents et d'amélioration continue.

4.2.6 Contrôle et audit

Mesures de cybersécurité pour contrôler la conformité de l'IT et de l'OT à la politique de sécurité des systèmes d'information et aux meilleures pratiques de sécurité.

OP 19 Effectuer régulièrement des audits de cybersécurité (tests de pénétration, équipe rouge, etc.) pour vérifier l'application et l'efficacité des mesures de sécurité et évaluer le niveau de sécurité des systèmes portuaires.

OP 20 Effectuer des révisions périodiques des règles de réseau, des privilèges de contrôle d'accès et des configurations d'actifs.

4.2.7 Protection physique IT et OT

Mesures de cybersécurité pour empêcher tout accès physique non autorisé aux systèmes informatiques et OT.

OP 21 S'assurer que les systèmes informatiques et OT hébergés dans le port sont protégés conformément aux meilleures pratiques établies en matière de sécurité (détection d'incendie, climatisation, etc.) et de sécurité (contrôle d'accès, vidéosurveillance, etc.).

OP 22 Garder la traçabilité de toutes les opérations de maintenance effectuées sur les systèmes physiques IT et OT.

4.3 Pratiques et mesures techniques

Les ports doivent appliquer plusieurs mesures techniques afin de prévenir les cyber-attaques sur les systèmes informatiques ou industriels des ports, détecter et réagir à toute attaque et être résilients en cas d'impact majeur d'une cyberattaque.

4.3.1 Sécurité du réseau

Mesures de cybersécurité pour éviter tout accès non autorisé aux systèmes portuaires, atténuer la propagation des incidents de sécurité informatique au sein des systèmes ou sous-systèmes et protéger les systèmes contre les accès non autorisés.

TP 01 Définir une architecture de segmentation de réseau pour limiter la propagation des attaques au sein des systèmes portuaires et éviter un accès direct depuis Internet à des systèmes portuaires très critiques tels que VTS / VTMIS et des systèmes de sécurité.

TP 02 Effectuer des analyses de réseau régulières pour détecter les réseaux non autorisés et malveillants (WIFI par exemple) ainsi que les terminaux utilisant des ponts entre deux zones séparées (avec des interfaces dans deux zones réseau par exemple).

TP 03 Définir la sécurité périmétrique, avec des règles de filtrage.

4.3.2 Contrôle d'accès

Mesures de cybersécurité pour garantir un accès légitime aux systèmes portuaires.

TP 04 Mettre en place des outils centralisés pour gérer les identités et les droits d'accès aux systèmes portuaires. Si différents outils sont mis en place, en raison de la diversité des acteurs portuaires (Autorités Portuaires, opérateurs de terminaux, collectivités locales, tiers, etc.) et de leurs systèmes, un approvisionnement automatique ou manuel peut être défini.

TP 05 Définir une stratégie de gestion des identités et des accès (« IAM ») et ses processus associés pour gérer le cycle de vie des identités et de leurs droits d'accès (désactivation automatique des comptes, examen régulier, principe du moindre privilège et séparation des tâches, directives relatives aux mots de passe, etc.). Cette stratégie doit être, autant que possible, construite en commun avec les acteurs de l'écosystème portuaire.

TP 06 Interdire autant que possible l'utilisation de comptes génériques, en imposant des comptes uniques et individuels dans tous les systèmes portuaires, en particulier pour les systèmes sensibles (PCS, CCS, TOS, VTS / VTMIS, systèmes de sécurité).

TP 07 Appliquer, dans la mesure du possible, les politiques et règles de complexité des mots de passe pour les systèmes.

TP 08 Mettre en œuvre des mécanismes d'authentification multifactorielle pour les comptes accédant aux applications critiques (en particulier pour PCS, CCS, TOS, VTS / VTMIS) et aux données (données personnelles, données opérationnelles sensibles telles que des informations détaillées sur les navires, les marchandises dangereuses et le fret), et en cas d'environnements pauvres ou non protégés (accès externe via Internet par exemple, accès tiers à partir d'autres réseaux d'entreprise, etc.).

TP 09 Considérer l'accès physique dans le cycle de vie de l'accès (installations portuaires, zone portuaire, bâtiments, etc.) et définir des mesures spécifiques pour l'accès à distance.

TP 10 Effectuer régulièrement des révisions des comptes et des droits d'accès pour s'assurer que les accès sont toujours légitimes, en particulier pour les comptes qui ont accès à des données sensibles (données personnelles, données opérationnelles sensibles, informations sur les marchandises dangereuses, etc.).

4.3.3 Administration et gestion de la configuration

Mesures de cybersécurité pour assurer une administration sécurisée des actifs informatiques et industriels.

TP 11 Définir la politique et les règles d'installation et de configuration et établir des bases de sécurité pour installer uniquement les services et fonctionnalités nécessaires et autoriser l'équipement essentiel pour la sécurité et le fonctionnement des systèmes portuaires.

TP 12 Configurer des comptes spécifiques uniquement utilisés par les administrateurs pour effectuer les opérations d'administration (installation, configuration, maintenance, supervision, etc.).

TP 13 Définir le processus de gestion des comptes privilèges (« PAM »), les exigences de sécurité sur ces comptes et les règles pour gérer leur cycle de vie. Faites particulièrement respecter ce processus pour les tiers qui supervisent les opérations d'administration.

TP 14 Mettre en place, autant que possible, des réseaux d'administration dédiés pour créer des zones sûres, en priorité pour les systèmes critiques (notamment pour les VTS / VTMIS, les systèmes radio, les systèmes de sécurité, etc.).

4.3.4 Gestion des menaces

Mesures de cybersécurité pour protéger tous les systèmes contre les logiciels malveillants ou les virus.

TP 15 S'assurer que l'anti-malware, l'anti-spam et l'antivirus sont installés et à jour sur tous les systèmes de port, y compris les ordinateurs de bureau et les serveurs.

4.3.5 Sécurité de l'informatique en nuage (« cloud »)

Mesures de cybersécurité pour protéger l'environnement de l'informatique en nuage (« cloud ») dans les ports.

L'informatique en nuage (« cloud ») fait l'objet d'un référentiel spécifique ANSSI (Secnumcloud).

TP 16 Définir une méthode d'évaluation de la sécurité de l'informatique en nuage (« cloud ») pour évaluer l'impact et les risques du choix de solutions cloud en tenant compte des lois et réglementations applicables.

TP 17 Inclure autant que possible les aspects de sécurité et de disponibilité dans les accords avec les fournisseurs de sécurité de l'informatique en nuage (« cloud »).

TP 18 Essayer d'inclure, autant que possible, des solutions de l'informatique en nuage (« cloud ») dans les mécanismes de détection et de réponse.

4.3.6 Sécurité de machine à machine

Mesures de cybersécurité pour sécuriser les échanges de machine à machine.

TP 19 Implémenter des mécanismes pour sécuriser les échanges de machine à machine (y compris les messages EDI et les API principalement utilisés avec des parties prenantes externes, telles que les compagnies maritimes) et assurer l'authentification mutuelle, l'intégrité et la confidentialité avec les systèmes portuaires tels que le cryptage, l'ICP ou certificats numériques, contrôles d'intégrité, signature numérique, horodatage, en particulier lorsque les échanges se font sur Internet.

TP 20 Utiliser des protocoles de communication qui incluent une fonctionnalité pour détecter si tout ou partie d'un message est une répétition non autorisée d'un message précédent.

4.3.7 Protection des données

Mesures de cybersécurité pour protéger les données au repos, en transit ou utilisées dans les systèmes portuaires.

TP 21 Mettre en œuvre des procédures et mécanismes de cryptographie pour protéger la confidentialité, l'authenticité et / ou l'intégrité des données dans les systèmes portuaires (au repos, en transit ou en cours d'utilisation). Cette mesure sera mise en œuvre en fonction de la classification des données effectuée.

TP 22 Anonymiser et sécuriser toutes les données personnelles directes ou indirectes traitées au sein de l'entreprise, par ex. grâce au contrôle d'accès et au chiffrement basés sur les rôles, après avoir pris en compte toutes les exigences légales pertinentes.

4.3.8 Gestion des mises à jour

Mesures de cybersécurité pour assurer la mise à jour des systèmes.

TP 23 Définir un processus de gestion des mises à jour pour s'assurer que les actifs informatiques et industriels du port sont à jour et, si cela n'est pas possible, appliquer des mesures compensatoires (séparation du réseau, durcissement des comptes, etc.), en particulier pour les systèmes hérités (systèmes industriels sans mise à jour possible, applications obsolètes mais critiques, etc.).

TP 24 Vérifier l'authenticité et l'intégrité des logiciels/micrologiciels des terminaux et assurez un contrôle strict de la mise à jour.

TP 25 Vérifier la source de la mise à jour et exécutez les procédures de mise à jour automatique uniquement si elles sont basées sur l'analyse des risques.

4.3.9 Détection et surveillance

Mesures de cybersécurité pour assurer la santé des actifs informatiques et OT et détecter toute cyberattaque.

TP 26 Surveiller la disponibilité des systèmes et appareils portuaires en temps réel, lorsque cela est techniquement possible, en se concentrant d'abord sur les systèmes et appareils critiques tels que les postes de travail d'administration, les systèmes radio et les appareils terminaux, les VTS / VTMIS, les systèmes radar ou la sécurité systèmes et terminaux industriels, la bande GPS/GNSS, etc.

TP 27 Configurer un système de journalisation pour enregistrer les événements liés, au moins, à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, aux modifications des règles de sécurité et au fonctionnement des systèmes portuaires.

TP 28 Mettre en place des systèmes de corrélation et d'analyse des journaux pour détecter les événements et contribuer à la détection des incidents de cybersécurité.

4.3.10 Sécurité des systèmes de contrôle industriels

Mesures de cybersécurité spécifiques aux systèmes industriels.

Les règles de l'arrêté du 14 septembre 2018 ne mentionnent pas explicitement les systèmes de contrôle industriels (« ICS »). Elles s'appliquent à tout type d'environnement (OT comme IT) et les éventuelles difficultés de mise en œuvre des mesures sur les systèmes OT sont couvertes par les exceptions introduites dans certaines règles sous une formulation du type : « lorsque… ne peut pas / ne permet pas … » et l'opérateur doit alors décrire les mesures complémentaires.

Les règles d'hygiène ne font pas non plus de focus sur l'OT, mais des guides ANSSI spécifiques OT existent.

TP 29 Prendre en compte les systèmes industriels dans toutes les mesures de sécurité définies dans ce rapport pour sécuriser autant que possible les systèmes et réseaux de contrôle industriels. Si celles-ci ne peuvent être appliquées, définir et mettre en œuvre des mesures compensatoires (ségrégation du réseau, durcissement des comptes, etc.).

TP 30 Assurer la segmentation du réseau entre les systèmes informatiques et industriels.

TP 31 Penser à mettre en place des mesures de sécurité spécifiques lors de la mise en œuvre de l'IoT.

4.3.11 Sauvegarde et restauration

Mesures de cybersécurité pour assurer la récupération des systèmes en cas d'incident, liées aux processus de résilience définis.

TP 32	Configurer des sauvegardes et s’assurer qu'elles sont régulièrement maintenues et testées, en particulier pour la plupart des systèmes centraux et critiques, comme Active Directory, PCS, CCS, TOS, etc.

5. PLANIFIER LA MISE EN ŒUVRE DE SES ACTIONS

Ce guide vous propose un exemple de chronologie simplifiée de mise en œuvre des nombreuses actions à réaliser pour améliorer la sécurité d'un SI. Face à l'importance de cette tâche, nous vous proposons ce fil conducteur qui vous permettra d'améliorer progressivement votre niveau de maturité en matière de cybersécurité. Cette progression est basée sur les 6 niveaux de maturité définis dans le guide ANSSI « Maturité SSI » auquel a été rajouté un niveau 0.

Ainsi, vous pouvez d'une part évaluer le niveau de maturité de votre organisme en vérifiant les actions déjà mises en œuvre et d'autre part identifier les actions nécessaires pour atteindre le niveau suivant.

Bien entendu, un niveau est atteint lorsque les actions présentées sont toutes et totalement appliquées sur l'ensemble du SI.

Les actions décrites ici, sont volontairement simplifiées afin de clarifier le cheminement de la mise en œuvre des mesures de sécurité en marquant les points de passages obligés. Chacune d'elles contribuent à la réussite de la mise en place des mesures de cybersécurité décrites au chapitre 4.

Chaque niveau de maturité SSI représente la manière dont une organisation exécute, contrôle, maintient et assure le suivi des processus SSI.

A noter qu'un guide de l'ENISA propose un modèle de maturité à trois niveaux : il décrit pour chaque mesure de sécurité, des exemples d'implémentation, du moins formel (niveau 1) au plus formel (niveau 3). La méthode EBIOIS RM (cf page 28 des fiches méthode) propose également une métrique de cotation pour la maturité cyber en quatre niveaux (du moins formel au plus formel).

Niveau 0. Pratique inexistante ou incomplète : pratiques de base éventuellement mises en œuvre et le besoin n'est pas reconnu.

- *Protection des postes de travail par un antivirus mis à jour quotidiennement*
- *Correctifs de sécurité appliqués sur les postes de travail*
- *Mot de passe obligatoire pour s'authentifier*
- *Plan d'adressage IP du réseau de l'entreprise, conforme à la réalité*
- *Fiche « départ agent » pour surveiller les droits et les matériels*

Niveau 1. Pratique informelle : actions isolées mises en œuvre de manière informelle et réactive sur l'initiative de ceux qui estiment en avoir besoin.

- *Droits d'accès aux ressources du réseau sont définis et appliqués*
- *Procédure d'alerte ou de signalement connue des utilisateurs (hotline par exemple)*
- *Description des étapes de mise à jour régulière ou d'urgence des correctifs de sécurité sur tous les équipements*
- *Filtrage Web mis en place*
- *Protection des postes de travail par un antispam*

Niveau 2. Pratique répétable et suivie : des actions reproductibles mises en œuvre de façon planifiée et suivie, avec un support relatif de l'organisme.

Les actions sont planifiées et sont réalisées par une personne qui possède des compétences en SSI. Certaines pratiques sont formalisées, ce qui permet la duplication et la réutilisation (éventuellement par une autre personne). Des mesures qualitatives sont réalisées (indicateurs simples sur les résultats). Les autorités compétentes sont tenues informées des mesures effectuées.

- *Comptes d'ouverture de session nominatifs et individuels*
- *Formalisation de la responsabilisation des acteurs de la chaine SSI (directeurs, administrateurs techniques et fonctionnels) avec des rôles séparés (décision, exécution) et signature des habilitations*
- *Comptes administrateurs dédiés pour les accès privilégiés (serveurs, équipements industriels)*
- *Suppression des comptes génériques*
- *Procédure d'autorisation des accès hors applicatif*
- *Procédure d'autorisation des accès intervention télémaintenance*
- *Top 10 de l'OWASP appliqué par les développeurs*
- *Préférence pour les protocoles sécurisés (HTTPS, SSH, FTPS, POPS)*
- *Validation par la direction de la « charte informatique », annexe du règlement intérieur signée par les utilisateurs*
- *Sensibilisation des utilisateurs des moyens informatiques aux attaques SSI (mails piégés, ingénierie sociale …) et formation aux bonnes pratiques (mot de passe, sauvegardes, réseaux sociaux …).*

Niveau 3. Processus défini : la standardisation de pratiques.

Les actions précédemment décrites sont toutes réalisées conformément à un processus défini (ex : adaptation au contexte, emploi d'une méthode), standardisé (commun à tout l'organisme) et formalisé (existence d'une documentation). Le processus SSI est bien compris autant par le management que par les exécutants.

- *Ressources, moyens sont affectés à la SSI*
- *Formations nécessaires pour les administrateurs techniques afin d'obtenir les certifications ISO2700x et les qualifications sur les outils informatiques en production.*
- *Politique de Sécurité des Systèmes d'Information (PSSI) conforme au cadre juridique applicable, validée par la direction.*
- *Systèmes sensibles : audits de sécurité, tests intrusion, analyse de risques, homologation*
- *Surveillance des accès en télémaintenance*
- *PCA et PRA formalisés*
- *Produits informatiques avec visas de sécurité au niveau adéquat*
- *Politique de « privilèges minimaux » sur les postes de travail*
- *Solution sécurisée de partage de fichier*
- *Applications, lors de chaque évolution du SI, des recommandations techniques et organisationnelles décrites dans les guides de l'ANSSI*
- *Protection du réseau par pare-feu et segmentation en VLAN*

Niveau 4. Processus contrôlé : la mesure quantitative.

La cybersécurité devient un avantage compétitif. Le processus est coordonné dans tout le périmètre choisi et pour chaque exécution. Des mesures quantitatives sont régulièrement effectuées (en termes de performance). Les mesures effectuées (indicateurs qualitatifs et quantitatifs) sont analysées et des améliorations sont apportées au processus.

- *Supervision managée des équipements en temps réel*
- *Mise en place d'un SOC et d'un SIEM*
- *Obtention par les administrateurs techniques des certifications et les qualifications sur les outils informatiques en production*
- *Cloisonnement vie privée / vie professionnelle*
- *Campagnes de faux mails piégés*
- *Données classifiées protégées selon l'IGI 1300*
- *Exercice gestion de crise et création de la cellule de crise cyber*
- *Cartographie du SI, de ses interactions et de ses flux*
- *Authentification forte (certificats, OTP, MFA, …)*
- *Mise à jour et suivi des indicateurs SSI*
- *Accès au SI depuis l'extérieur par VPN*
- *Isolation des systèmes industriels du réseau interne et de l'Internet*
- *Blocage 802.1x des prises et des équipements connectés (caméras, photocopieurs, imprimantes, etc.)*
- *Chiffrement des postes de travail ou virtualisation*

Niveau 5. Processus optimisé : l'amélioration continue.

Le processus est adapté de façon dynamique à la situation. L'analyse des mesures effectuées est définie, standardisée et formalisée. L'amélioration du processus est définie, standardisée et formalisée.

- *Chaque évolution du SI est journalisée*

- *Chaque action précédemment décrite fait l'objet d'une revue dont la fréquence est définie dans le cadre d'une démarche d'amélioration continue type PDCA.*

« Les 7 couches du modèle CISO* »

Le modèle « CISO » constitue une proposition d'actions, regroupées par fonctions SSI, pouvant être mise en œuvre suite à l'analyse effectuée en se servant des parties 3 et 4.

7	**Supervision**	Surveillance des accès en télémaintenance ; supervision managée des équipements en temps réel ; mise en place d'un SOC et d'un SIEM.
6	**Gouvernance**	Formalisation de la responsabilisation des acteurs de la chaine SSI (directeurs, administrateurs techniques et fonctionnels) avec des rôles séparés (décision, exécution) et signature des habilitations ; validation par la direction de la « charte informatique », annexe du règlement intérieur signée par les utilisateurs ; ressources, moyens sont affectés à la SSI ; formations nécessaires pour les administrateurs techniques afin d'obtenir les certifications ISO2700x et les qualifications sur les outils informatiques en production ; politique de Sécurité des Systèmes d'Information (PSSI) conforme au cadre juridique applicable, validée par la direction.
5	**Procédures**	Procédure (ou processus) de gestion des droits d'accès (arrivée / départ / modification) ; procédure d'autorisation des accès hors applicatif ; procédure d'autorisation des accès intervention télémaintenance ; systèmes sensibles (audits de sécurité, tests intrusion, analyse de risques, homologation) ; produits informatiques avec visas de sécurité au niveau adéquat ; applications, lors de chaque évolution du SI, des recommandations techniques et organisationnelles décrites dans les guides de l'ANSSI ; données classifiées protégées selon l'instruction générale interministérielle 1300 ; exercice gestion de crise et création de la cellule de crise cyber ; mise à jour et suivi des indicateurs SSI.
4	**Utilisateurs**	Définition et mise en place d'une politique de mot e passe (ex : mot de passe obligatoire pour s'authentifier) ; procédure d'alerte ou de signalement connue des utilisateurs (hotline par exemple) ; comptes d'ouverture de session nominatifs et individuels ; sensibilisation des utilisateurs des moyens informatiques aux attaques SSI (incluant des tests de faux mails piégés « phishing », ingénierie sociale …) et formation aux bonnes pratiques (mot de passe, sauvegardes, réseaux sociaux…) ; les administrateurs techniques ont obtenu les certifications et les qualifications sur les outils informatiques en production ; cloisonnement vie privée / vie professionnelle.
3	**Applications**	Top 10 de l'OWASP appliqué par les développeurs ; authentification forte (certificats, OTP, MFA, etc.).
2	**Systèmes**	Protection des postes de travail par un antivirus mis à jour quotidiennement ; correctifs de sécurité appliqués sur les postes de travail ; droits d'accès aux ressources du réseau sont définis et appliqués ; description des étapes de mise à jour régulière ou d'urgence des correctifs de sécurité sur tous les équipements ; protection des postes de travail par un antispam ; comptes administrateurs dédiés pour les accès privilégiés (serveurs, équipements industriels) ; suppression des comptes génériques, PCA et PRA formalisés, Solution sécurisée de partage de fichier ; cartographie du SI, de ses interactions et de ses flux ; chiffrement des postes de travail ou virtualisation.
1	**Réseaux**	Plan d'adressage IP du réseau de l'entreprise, conforme à la réalité ; filtrage Web mis en place ; préférence pour les protocoles sécurisés (HTTPS, SSH, FTPS, POPS) ; protection du réseau par pare-feu et segmentation en VLAN ; accès au SI depuis l'extérieur par VPN, Isolation des systèmes industriels du réseau interne et de l'Internet ; blocage 802.1x des prises et des équipements connectés (caméras, photocopieurs, imprimantes…).

*(CISO) Chief Information Security Officer - (RSSI) Responsable de la Sécurité des Systèmes d'Information.

6. GÉRER LES CYBERINCIDENTS AVÉRÉS

6.1 Anticiper la survenue des cyberincidents

6.1.1 Mettre en œuvre un plan de réponse aux cyberattaques

Il est important de prévoir un plan de réponse composé par :

- un plan de continuité informatique permettant à votre organisation de continuer à fonctionner quand survient une altération du système d'information, comprenant par exemple des moyens de communication de secours
- un plan de reprise informatique visant à remettre en service les systèmes d'information qui ont dysfonctionné. Il doit notamment prévoir la restauration des systèmes et des données.

Ces plans doivent régulièrement être actualisés et éprouvés à l'aide d'exercices impliquant l'ensemble des acteurs et des domaines fonctionnels.

6.1.2 Penser sa stratégie de communication de crise cyber

L'élaboration d'une stratégie de communication de crise adaptée repose sur la mise en relation préalable des équipes « métiers » et des personnes en charge de la sécurité numérique, qui ensemble, peuvent élaborer une stratégie qui prend en compte :

- la cartographie des publics et les objectifs de communication associés : public interne, clients, partenaires, autorités, grand public/médias ;
- la cartographie des parties prenantes de la communication avec qui il sera nécessaire de se coordonner : prestataires, filiales, autorités, etc. ;

- les actions à mener à court, moyen et long terme vis-à-vis de l'externe (relations presse, communication web, etc.) comme des collaborateurs.

- penser à élaborer une communication de crise aussi bien externe qu'interne ;

- tester lors des exercices la stratégie de communication.

6.2 Réagir de manière adaptée aux cyberincidents

6.2.1 Adopter les bons réflexes

Lors de tout cyber-incident le premier réflexe est d'ouvrir une main courante permettant de tracer les actions et les évènements liés à l'incident. Chaque entrée de ce document doit contenir, a minima :

- l'heure et la date de l'action ou de l'événement ;
- le nom de la personne à l'origine de cette action ou ayant informé sur l'événement ;
- la description de l'action ou de l'événement.

Consultez la note d'information « Les bons réflexes en cas d'intrusion sur un système d'information » sur le site du CERT-FR.

Sollicitez sinon l'ANF en cas de brouillage sur les bandes radio / radar / GNSS.

6.2.2 Piloter la gestion de la crise cyber

Les enjeux induits par une telle attaque vont bien au-delà de la perte de données ou du paiement d'une rançon. C'est pourquoi il est recommandé de mettre en place une cellule de crise au plus haut niveau de l'organisation, indépendante des groupes de travail opérationnels qui auront des responsabilités de pilotage et d'exécution.
Cette cellule aura pour objectif :

- de répondre aux enjeux de niveau stratégique de la crise en établissant (stratégies de communication interne comme externe, réunir les éléments à fournir en vue de la judiciarisation.

- de demander l'appui du délégué à la protection des données (DPO)

- d'identifier les impacts de ces dysfonctionnements sur les activités de l'organisation.

6.2.3 Signaler le cyber-incident ou la cyber-attaque

Les éléments suivants vous aideront à avoir les bons réflexes et à contacter les bons correspondants.

Vous êtes un particulier, TPE/PME ou une collectivité territoriale ?

Vous pouvez contacter le dispositif d'assistance aux victimes d'actes de cybermalveillance : « cybermalveillance.gouv.fr **»**

Vous êtes un opérateur d'importance vitale (OIV) ?

Retrouvez le formulaire de déclaration d'incident à adresser à l'ANSSI dans la rubrique « Cybersécurité des OIV »
Vous êtes un opérateur de services essentiels (OSE) ?

Retrouvez le formulaire de déclaration d'incident à adresser à l'ANSSI dans la rubrique « Cybersécurité des OSE »

Ne pas payer la rançon

En cas de cyberincident généré par un rançongiciel, il est recommandé de ne jamais payer la rançon. Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux. De plus, le paiement de la rançon n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels.

Par ailleurs, l'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus (exemple : un fichier de base de données).

6.2.4 Trouver l'assistance technique

Il est possible de faire appel à des prestataires spécialisés dans la réponse aux incidents de sécurité. Le Gouvernement a mis en place la plateforme « cybermalveillance.gouv.fr » qui permet d'entrer en contact avec des prestataires de proximité.

Retrouvez la liste des prestataires de réponse aux incidents ici.

6.2.5 Déposer plainte

La cybercriminalité recouvre les infractions parmi lesquelles :

- les atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.), autrement dit les cyberattaques, sanctionnées par les articles 323-1 à 323-8 du code pénal, notamment l'accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal) ;
- les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, sanctionnées par les articles 226-16 à 226-24 du code pénal, notamment la collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal) ;
- les atteintes aux personnes, sanctionnées notamment par les articles 226-4-1 (usurpation d'identité) et 222-17 (menaces) du code pénal ;
- les escroqueries (telles que l'hameçonnage, « phishing »), sanctionnées par les articles 313-1 du code pénal, ;
- la contrefaçon et l'usage frauduleux de moyens de paiement, sanctionnés notamment par les articles L. 163-3 et L. 163-4 du code monétaire et financier ;
- la contrefaçon des marques (logos, signes, emblèmes, etc.) utilisées lors de l'hameçonnage, sanctionnée par les articles L. 713-2 et L. 713-3 du code de la propriété intellectuelle.

Il est donc recommandé de porter plainte directement auprès des services de police ou de gendarmerie - y compris maritime - le plus proche de l'entreprise ou par courrier adressé au Procureur de la République du tribunal judiciaire du ressort géographique de l'entreprise.

Les éléments suivants peuvent être demandés ou pourront être recherchés dans le cadre de l'enquête. En fonction du profil de votre entité, ils peuvent diverger :

- le détail et la chronologie des événements relatant l'incident (la main courante), notamment la date de la demande de rançon ;
- les emplacements des appareils potentiellement infectés ;
- les journaux de sécurité associés à l'incident ;

- l'analyse technique de l'attaque ;
- la collecte d'échantillons de fichiers chiffrés ;
- la préservation des supports ou des machines (quand c'est possible) sur lesquels le rançongiciel s'est exécuté (disque système) ;
- les adresses de messagerie électronique et adresses de crypto-monnaie fournies par les cybercriminels ;
- le texte de demande de rançon ;
- les coordonnées des témoins de l'incident.

Le dépôt de plainte doit être réalisé au nom de l'entité. Si l'opération est confiée à un collaborateur, il sera nécessaire de préparer une délégation de pouvoir pour cette personne, signée par un représentant légal de la personne morale afin de permettre le dépôt de plainte.

Le ministère de l'Intérieur ouvrira une plateforme de plainte en ligne en matière d'escroqueries sur Internet appelée « THESEE ».

Par ailleurs, en cas de fuite de données personnelles, il faut signaler la cyberattaque à la Commission nationale de l'informatique et des libertés (CNIL) dans les 72h suivant sa constatation, conformément à l'article 33 du règlement général sur la protection des données (RGPD). Un formulaire est téléchargeable sur le site Internet de la CNIL.

Lorsque la vie privée d'une personne est grandement menacée, l'article 34 du RGPD enjoint à l'entreprise d'alerter la personne concernée de la violation de ses données personnelles.

CONCLUSION

Alors que les ports subissent leur transformation numérique, la cybersécurité doit être considérée non seulement comme un facteur clé à prendre en compte pour suivre le rythme des évolutions techniques, mais aussi comme un catalyseur de nouveaux développements et d'automatisation. Compte tenu de la complexité du paysage portuaire en termes de parties prenantes impliquées et de flux de communication et d'interactions système, mais également en termes d'évolution de l'environnement informatique et OT, il ne s'agit en aucun cas d'une tâche facile ou directe.

Comme document de référence des acteurs portuaires impliqués dans la cybersécurité portuaire, ce guide concourt à leur sensibilisation et à insuffler une culture de cybersécurité, tant au niveau des décideurs que des personnels. Les premiers augmenteront probablement l'attention stratégique accordée aux risques de cybersécurité qui se traduira par des investissements plus importants et davantage de ressources pour les atténuer, tandis que les seconds sont essentiels pour assurer la cybersécurité dans les opérations quotidiennes dans les ports. En effet, le secteur maritime est historiquement très conscient des questions de sûreté et de sécurité, mais la cybersécurité commence à peine être pleinement appréhendée par les acteurs qui doivent par ailleurs être formés, se former, afin de garantir une bonne compréhension des questions de cybersécurité et la capacité d'être vigilant aux enjeux de cybersécurité dans les opérations quotidiennes.

Ce guide permettra également de favoriser la collaboration entre les nombreuses parties prenantes impliquées dans les opérations portuaires (autorités portuaires, exploitants d'installations portuaires, opérateurs portuaires, société de pilotage, compagnies maritimes, etc.) autour des enjeux de cybsersécurité.

Néanmoins, les personnes responsables de la cybersécurité portuaire, à savoir les RSSI, DSI, responsables informatiques, etc. des autorités portuaires et des exploitants d'installations portuaires sont encouragées à aller au-delà des bonnes pratiques proposées dans le présent guide et à aborder également des sujets supplémentaires, tels que :

- la prise en compte de la sécurité dès la conception dans les applications, d'autant plus que les ports utilisent de nombreux systèmes, dont certains sont ouverts à des tiers pour l'échange de données. Toute vulnérabilité sur ces systèmes peut être une porte pour compromettre les systèmes portuaires ;

- le renforcement des capacités de détection et de réponse au niveau du port pour réagir le plus rapidement possible à toute cyberattaque avant qu'elle n'affecte le fonctionnement, la sûreté ou la sécurité du port. Les ports peuvent s'appuyer sur des mesures de détection simples telles que des alertes lorsqu'une action spécifique est effectuée (tentative d'authentification sur un actif très critique par exemple) ou rechercher des indicateurs de compromis (IOC), ou sur des méthodes plus complètes, utilisant l'apprentissage automatique pour corréler les informations et identifier les modèles compromettants. De telles initiatives ont déjà commencé à se développer au sein de l'écosystème portuaire.

- l'amélioration du partage d'informations entre les opérateurs portuaires (autorités portuaires, opérateurs de terminaux, etc.) et entre les opérateurs portuaires et les autres acteurs maritimes, tels que les compagnies maritimes. Le partage d'informations sur les menaces, les incidents et les bonnes pratiques est essentiel pour améliorer la posture globale de cybersécurité du secteur et plusieurs modèles éprouvés, tels que les ISAC, peuvent être adaptés pour fournir des résultats tangibles.

- le traitement de la cybersécurité dans la chaîne d'approvisionnement. Bien qu'une approche holistique pour résoudre ce problème complexe ne soit pas une tâche facile, plusieurs bonnes pratiques peuvent être adoptées ou étudiées, y compris la certification de cybersécurité des composants critiques, des obligations de fournisseur bien définies pour l'ensemble du cycle de vie des produits / services (ex. : gestion des vulnérabilités, correctifs), des dispositions spécifiques pour la gestion de la chaîne d'approvisionnement, etc.

- l'intégration des interdépendances des risques de cybersécurité dans le processus global de gestion des cyber risques pour tenir compte des interconnexions multiples et complexes des ports avec d'autres secteurs.

- l'attention à porter sur le champ connexe du brouillage radio des bandes de fréquences.

LIENS UTILES

État de la menace sur les rançongiciels de l'ANSSI :
cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001

Guide d'hygiène informatique de l'ANSSI :
ssi.gouv.fr/guide/guide-dhygiene-informatique

Guide sur la maîtrise des risques numériques de l'ANSSI et de l'AMRAE :
ssi.gouv.fr/uploads/2019/11/anssi_amraeguide-maitrise_risque_numerique-atout_confiance.pdf

Guide EBIOS Risk manager et son supplément :
ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide

Liste des prestataires de confiance qualifiés par l'ANSSI :
ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/

Fiche sur « les mises à jour » de cybermalveillance :
cybermalveillance.gouv.fr/medias/2020/04/fiche_mises_a_jour.pdf

Fiche sur « les sauvegardes » de cybermalveillance :
cybermalveillance.gouv.fr/medias/2019/11/Les-sauvegardes.pdf

Fiche sur « les rançongiciels » de cybermalveillance :
ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/

Guide ANSSI pour la réalisation d'exercice de crise cyber :
ssi.gouv.fr/uploads/2020/10/anssi-guide-organiser-un-exercice-de-gestion-de-crise-cyber-v1.0.pdf

Guide d'élaboration d'une PSSI :
ssi.gouv.fr/entreprise/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/

Guide d'élaboration d'une charte informatique pour les PME et ETI :
ssi.gouv.fr/entreprise/guide/guide-delaboration-dune-charte-dutilisation-des-moyens-informatiques-et-des-outils-numeriques/

Guide à l'usage des professionnels en déplacement :
ssi.gouv.fr/entreprise/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/

Comprendre et anticiper les attaques DDOS :
ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les-attaques-ddos/

Mise en place d'une politique de pare-feu :
ssi.gouv.fr/entreprise/guide/recommandations-pour-la-definition-dune-politique-de-filtrage-reseau-dun-pare-feu/

Guide pour durcir les postes de travail et les serveurs Windows :
ssi.gouv.fr/uploads/2016/03/np_emet_notetech.pdf

Définir l'architecture d'interconnexion d'un SI à Internet :
ssi.gouv.fr/entreprise/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/

BIBLIOGRAPHIE

Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI, Guide « La cybersécurité des systèmes industriels » - Cas pratiques (Version 1.0), Juin 2012.

Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI, Guide « La cybersécurité des systèmes industriels » - Maîtriser la SSI pour les systèmes industriels (Version 1.0), Juin 2012.

Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI, Guide « La cybersécurité des systèmes industriels » - Mesures détaillées (Version 1.0), Janvier 2014.

Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI, Guide « La cybersécurité des systèmes industriels » - Méthode de classification et mesures principales (Version 1.0), Janvier 2014.

Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI, Guide d'hygiène informatique – Renforcer la sécurité de son système d'information en 42 mesures (Version 2.0), Septembre 2017.

European Commission, Transport cybersecurity toolkit, 16 décembre 2020 https://ec.europa.eu/transport/sites/transport/files/cybersecurity-toolkit_en.pdf

European Union Agency for Cybersecurity – ENISA, Port Cybersecurity (dont sont issues les figures du present guide) – Good practices for cybersecurity in the maritime sector, Novembre 2019.

European Union Agency for Cybersecurity – ENISA, Guidelines – Cyber Risk Management for port, Décembre 2020.

Gouvernement - Stratégie nationale portuaire – Pour un réseau de ports au coeur des chaînes logistiques, du développement économique et des transitions écologique et numérique, Janvier 2021.

GOUVERNEMENT

Liberté
Égalité
Fraternité

Juin 2021