European Commission

Mécanisme de suivi, de soutien et d'évaluation du programme Routes Maritimes Critiques (CRIMSON III)

La cybersécurité dans les infrastructures maritimes critiques

Réflexion sur les ports africains

Service des instruments de politique étrangère

COMMISSION EUROPÉENNE
Office de coopération EuropeAid
Instrument de stabilité/ Contrat no. N° IFS/2019/410-525

Soumis à :
Ondrej Vosatka
Service des instruments de politique étrangère (IPE)
IPE.1 - Paix et stabilité - Menaces et défis mondiaux et transrégionaux
SEAE 02/9A Rond-Point Schuman, Bruxelles

Contrat no. N° IFS/2019/410-525

Date : 20/04/2023

Auteurs :
Nineta Polemi, Professeure en cybersécurité, dpolemi@gmail.com
Christophe Van Maele, Expert maritime, cvanmaele@portconsult.eu

Le travail a été coordonné par Evelyn Vancollie, Coordinatrice du projet CRIMSON.

Cette étude est financée par le Service des instruments de politique étrangère (IPE) de l'Union européenne par le biais du mécanisme de suivi, de soutien et d'évaluation des Routes Maritimes Critiques (CRIMSON III), et mis en œuvre par RUSI Europe. Il a bénéficié du soutien du réseau CyberNet de l'UE.

Ce rapport a été réalisé avec le concours de l'UE. Le contenu de ce rapport relève de la seule responsabilité des auteurs et ne peut en aucun cas être considéré comme reflétant le point de vue de l'UE.

Table des matières

Liste des acronymes 5

Liste des images 7

Résumé 8

1 Introduction 10

2 Un écosystème maritime complexe 11

3 L'Union européenne (UE) et les ports africains 14

3.1 Introduction 14

3.1.1 Les ports africains 15

3.1.2 Commerce maritime entre l'UE et l'Afrique 17

4 Concepts de sécurité maritime 19

4.1 Introduction 19

4.2 Concepts et terminologie de la sécurité 19

4.3 Technologies maritimes physiques et informatiques 20

4.3.1 Numérisation accélérée du secteur maritime 22

4.4 Incidents de sécurité et acteurs de la menace 22

4.4.1 Types d'attaquants 22

4.4.2 Incidents de sécurité 23

4.4.2.1 Accidents de sécurité 25

4.4.2.2 Cyberattaques 26

4.4.2.3 Attaques TI/TO 28

4.4.2.4 L'utilisation d'ordinateurs pour communiquer entre les parties prenantes permet d'agir efficacement et en temps réel lorsque cela est nécessaire. Chaîne d'approvisionnement et menaces hybrides 29

4.4.2.5 Vecteurs de menace 31

5 Normes et stratégies en matière de sécurité maritime 34

5.1 Introduction 34

5.1.1 Stratégie de sûreté maritime de l'Union européenne (SSMUE) 34

5.1.2 Normes en matière de sûreté maritime 35

5.1.2.1 Le code ISPS 35

5.1.2.2 Autres codes importants 38

5.1.3 Normes en matière de cybersécurité 39

5.1.3.1 Normes ISO pour la sécurité des IIC maritimes 39

5.1.3.2 Normes ISA, ANSI pour les ACS 40

5.1.3.3 Catégorisation des normes 40

5.2 Législation en matière de sûreté 42

5.3 Législation en matière de cybersécurité 44

6 Bonnes pratiques dans le domaine de la sécurité maritime 46

6.1 Introduction 46

6.2 Gouvernance de la sécurité maritime 46

6.3 Hygiène des opérateurs en matière de cybersécurité 47

6.4 Gestion de la sécurité maritime 48

6.4.1 Gestion de la sûreté (sécurité physique) 49

6.4.2 Gestion de la cybersécurité 55
6.5 La cyber-résilience maritime 58
6.6 Facteurs humains 59

7 Pratiques de sécurité portuaire en Afrique 61
7.1 Les ports du Golfe de Guinée 61
7.2 Organisation de la sécurité portuaire en Afrique 61
7.3 Initiatives internationales pour les ports africains 63
7.4 Les cyber-risques en Afrique 64

8 Conclusions 67

9 Recommandations 68
9.1 Recommandations aux ports d'Afrique subsaharienne 68
9.2 Recommandations aux acteurs maritimes africains 69
9.3 Soutien de la direction générale 69
9.4 Sensibilisation à la cybersécurité 70
9.5 Procédures, lignes directrices et instructions en matière de cybersécurité 70
9.6 Services et fonctions critiques de l'organisation 70
9.7 Évaluation des risques liés à la cybersécurité 70
9.8 Plan de gestion de la cybersécurité 70
9.9 Cybersécurité de la chaîne d'approvisionnement 70
9.10 Gestion des incidents, réponse et rétablissement 71
9.11 Normes et cadres en matière de cybersécurité 71
9.12 Recommandations générales pour les ports en matière de cybersécurité 71
9.13 Recommandations à l'UE : vers une collaboration stable entre l'UE et l'Afrique 73

10 Références bibliographiques 75

11 Annexes : Questionnaires portant sur la sécurité 78
11.1 Annexe A : Questionnaire sur la sensibilisation à la gouvernance de la sécurité 78
11.2 Annexe B : Questionnaire sur les pratiques de sécurité 82

Liste des acronymes

AESM	Agence européenne pour la sécurité maritime
AI	Intelligence artificielle
AIS	Système d'identification automatique
CCTV system	Système de télévision en circuit fermé
COP	Code de pratique
COS	Centre des opérations de sécurité
COSCO	China Ocean Shipping Company
CSA	Évaluation de la cybersécurité
CSIRT	Centre de réponse aux incidents de sécurité informatique
CSO	Agent de sûreté de la compagnie
CSP	Plan de cybersécurité
CYSO	Agent chargé de la cybersécurité
DA	Autorités compétentes
DDoS	Déni de service (distribué)
ECDIS	Système de visualisation des cartes électroniques et d'information
ENISA	Agence de l'Union européenne pour la cybersécurité
FSN	Fournisseurs de services numériques
GMN	Réseau mondial de MTCC
GNL	Gaz naturel liquéfié
IACS	Association internationale des sociétés de classification
IAPH	Association internationale des ports
Recueil IBC	Recueil international de règles relatives à la construction et à l'équipement des navires transportant des produits chimiques dangereux en vrac
IC	Infrastructure critique
ICS	Système de contrôle-commande industriel
IIC	Infrastructure d'information critique
Code IMDG	Code maritime international des marchandises dangereuses
Code IMSBC	Code maritime international des cargaisons solides en vrac
IoT	Internet des objets
ISAC	Centre d'analyse et de partage de l'information
ISC	Initiative sur la sécurité des conteneurs
ISM	Gestion internationale de la sécurité
ISPS	Code international pour la sûreté des navires et des installations portuaires
MSC	Compagnie maritime méditerranéenne
MTCC	Centre de coopération en matière de technologie maritime
NIS	Réseaux et systèmes d'information
Niveau de sûreté 1	Le niveau de sûreté 1 au titre du code ISPS définit les mesures de protection minimales appropriées
Niveau de sûreté 2	Le niveau de sûreté 2 au titre du code ISPS définit les mesures additionnelles à maintenir pendant une période déterminée en raison d'un risque accru d'incident de sûreté
Niveau de sûreté 3	Le niveau de sûreté 3 au titre du code ISPS prévoit l'activation de mesures spéciales à maintenir pendant une période limitée en cas de menace probable ou imminente

NLF	Nouveau cadre législatif
OIT	Organisation internationale du Travail
OMI	Organisation maritime internationale
OSE	Opérateurs de services essentiels
PCS	Système communautaire portuaire
PFSO – PSO	Agent de sûreté (de l'installation) portuaire
POP	Procédures opérationnelles permanentes
PSA – PFSA	Évaluation de la sûreté (de l'installation) portuaire
PSC	Régimes de contrôle par l'État du port
PSO - PFSO	Agent de sûreté (de l'installation) portuaire
PSP – PFSP	Plan de sûreté (de l'installation) portuaire
RA	Évaluation des risques
RFID	Identificateur de radiofréquence
RGPD	Règlement général sur la protection des données
RIB	Bateau pneumatique rigide
RM	Gestion des risques
RMF	Cadre de gestion des risques
RSSI	Responsable de la sécurité des systèmes d'information
SCADA	Système de supervision industrielle maritime
SCSO	Agent chargé de la cybersécurité des navires
SEAE	Service européen pour l'action extérieure
SeMS	Système de gestion de la sécurité
SGSI	Système de gestion de la sécurité de l'information
SMDSM	Système mondial de détresse et de sécurité en mer
SMS	Système de gestion de la sûreté
SOLAS	Sauvegarde de la vie humaine en mer
SSMUE	Stratégie de sûreté maritime de l'Union européenne
SSO	Agent de sûreté du navire
SSP	Plan de sûreté du navire
STCW	Formation des gens de mer, délivrance des brevets et veille
TI	Technologie de l'information
TIC	Technologies de l'information et de la communication
TO	Technologie opérationnelle
TOS	Système d'exploitation de terminal
YARIS	Réseau d'échange de l'architecture de Yaoundé

Liste des images

Image 1: Environnement maritime 11

Image 2: Ports africains 16

Image 3: La sécurité comprend la sûreté et la cybersécurité 19

Image 4: Taxonomie des installations des ports maritimes élaborée par l'ENISA 20

Image 5 : Technologies navales 21

Image 6: Technologies portuaires 22

Image 7: Taxonomie des attaques contre les chaînes d'approvisionnement proposée par l'ENISA. 31

Image 8: Taxonomie des normes de sécurité maritime 41

Image 9: Approche de la gestion de la sécurité par le BIMCO 49

Image 10: Matrice de l'appétit pour le risque 56

Image 11: Approche du BIMCO de la gestion de la cybersécurité 57

Image 12: Architecture de sécurité physique et informatique SAURON 58

Image 13: Résilience maritime 58

Image 14: Objectifs de sécurité de l'IET 59

Image 15: Région maritime du Golfe de Guinée 61

Image 16: Système TO de contrôle du périmètre 63

Résumé

Les ports commerciaux modernes sont des infrastructures critiques qui dépendent fortement des systèmes d'information. La sécurité d'un port repose donc sur l'intégrité des installations physiques et électroniques. Il a été prouvé que les ports deviennent des cibles pour les pirates informatiques. En effet, leurs attaques peuvent affecter à la fois les installations informatiques et physiques, et interrompre les opérations. Malgré ce constat, trop de ports disposent d'une cybersécurité inadéquate. Les menaces physiques, les incidents et les accidents qui touchent les installations physiques (terminaux, portes, bâtiments) des infrastructures maritimes, ou encore les menaces et les attaques informatiques qui touchent des installations telles que les systèmes communautaires portuaires et les systèmes de navigation peuvent compromettre les opérations maritimes, perturber les chaînes d'approvisionnement et porter un coup fatal au commerce et aux échanges internationaux.

Cette étude documentaire fournit une évaluation des concepts de sécurité maritime (sûreté et cybersécurité) pour les ports, ainsi que des normes, méthodologies, meilleures pratiques, outils et cadres de gestion de la sécurité. Elle analyse également les régimes juridiques et réglementaires existants. Par ailleurs, le rapport présente les cybermenaces et les attaques auxquelles l'écosystème maritime (ports, navires, compagnies maritimes, autorités, chaînes d'approvisionnement maritimes) doit faire face en raison d'une numérisation en plein essor. Les conséquences et l'impact de ces menaces sur les opérateurs maritimes, les parties prenantes, les économies et la sécurité nationale peuvent être considérables. Les normes, les stratégies ainsi que les instruments juridiques et politiques en matière de cybersécurité sont présentés dans ce document pour servir d'exemples d'efforts en vue de relever de manière globale les défis de la cybersécurité maritime. Cette étude s'efforce aussi de donner un aperçu des méthodologies, des outils et des lignes directrices en matière de gestion des risques basés sur les normes afin de sensibiliser les ports aux approches internationales existantes. Le respect des normes et des stratégies de sécurité existantes renforce la résilience des opérations internationales, des chaînes d'approvisionnement et du commerce.

Le rapport présente également le niveau de sensibilisation à la sécurité des ports d'Afrique subsaharienne par rapport aux efforts déployés en Europe. Les deux questionnaires en annexe, élaborés par les auteurs, peuvent être distribués aux acteurs maritimes africains afin qu'ils puissent évaluer eux-mêmes leur niveau de gouvernance de la sécurité (Annexe A) et leur niveau de maturité en matière de sensibilisation et de pratiques (Annexe B). Les questionnaires peuvent également être utilisés pour améliorer le niveau de préparation à la sécurité. Enfin, des recommandations pratiques sont formulées à l'attention de l'UE sur la manière d'établir de meilleures relations avec les ports africains afin de renforcer leurs capacités en matière de sécurité. Le rapport sert à alerter les ministères chargés des affaires maritimes et les gouvernements sur les questions qui doivent être prises en considération.

Le rapport contient des recommandations visant à améliorer de manière globale la sécurité dans les ports africains, mais également des recommandations spécifiques en matière de cybersécurité. D'un côté, la législation sur la cybersécurité doit être révisée au niveau

national. De l'autre, les directions générales des autorités portuaires doivent être encouragées à poursuivre leurs efforts en matière de gouvernance de la sécurité, y compris en termes de personnel et de ressources. Une formation de sensibilisation à la cybersécurité serait nécessaire pour tous les acteurs concernés et des équipes de cybersécurité devraient être constituées. Dans un premier temps, les auteurs du rapport recommandent de dresser un inventaire de toutes les installations critiques, y compris informatiques. Dans un second temps, une évaluation des risques permettrait d'identifier les cybermenaces, les risques et les vulnérabilités. Sur la base de ces éléments, il serait possible d'élaborer un plan de gestion de la cybersécurité dans lequel figurerait la gestion et la réponse à des incidents informatiques, ainsi que le rétablissement post-incident. Les fournisseurs d'équipements de cybersécurité peuvent avoir accès à distance aux équipements. Leur sécurité informatique devra également faire l'objet d'une évaluation. Il existe des normes et des compétences en matière de cybersécurité qui peuvent aider les ports à créer et à maintenir leur bouclier informatique.

Des recommandations sont également adressées à l'UE sur la manière de renforcer sa collaboration avec l'Afrique dans les domaines de la sécurité maritime, de la cybersécurité et de la sécurité des chaînes d'approvisionnement. L'UE devrait s'efforcer de mettre en place des collaborations stables entre les ministères chargés des transports maritimes, les agences de sécurité et les centres d'analyse et de partage de l'information maritime. L'UE devrait également chercher à combler l'écart en matière de compétences informatiques avec ses partenaires africains, y compris au moyen d'exercices concrets. Les centres d'opérations de sécurité maritime arrivent à anticiper et gérer efficacement les cyberattaques et les incidents de sécurité. Il serait possible de renforcer davantage la collaboration entre l'UE et l'Afrique grâce à un soutien transfrontalier visant à améliorer l'exploitation de ces centres. L'harmonisation des efforts de certification maritime, notamment par le biais d'évaluations et d'audits conjoints de la sécurité des équipements maritimes, serait également utile afin de garantir le respect de la confidentialité, la sécurité, la transparence, l'interopérabilité, la responsabilité et la conformité à la législation et aux lignes directrices internationales en matière de sécurité. Enfin, des analyses comparatives entre les ports de l'UE, de la région d'Afrique subsaharienne et d'autres régions du monde devraient permettre d'établir régulièrement des critères de référence. Il serait alors possible de mettre en évidence les approches communes fructueuses entre l'UE et l'Afrique en matière de sécurité et de cybersécurité, qui pourraient être émulées dans d'autres régions.

1 Introduction

Le secteur maritime soutient les entreprises et les économies grâce à la circulation des personnes et des biens vitaux, tels que l'énergie (transport de pétrole et de gaz) et les denrées alimentaires. L'économie dépend essentiellement de la sécurité physique et de la sûreté du transport maritime de marchandises et de passagers. Toutefois, étant donné que l'activité maritime repose de plus en plus sur les technologies de l'information et de la communication (TIC) pour optimiser ses opérations (de la navigation à la propulsion, en passant par la gestion du fret et les communications de contrôle du trafic), la cybersécurité est devenue une exigence essentielle. Ces dernières années, la crainte d'être la cible de cyberattaques fait peser une menace croissante qui s'étend à l'ensemble de l'écosystème maritime (des ports aux compagnies maritimes en passant par d'autres infrastructures critiques interconnectées, telles que les transports ou les autorités maritimes). L'interruption ou l'indisponibilité des capacités TIC maritimes pourrait avoir des conséquences désastreuses. Il est donc de plus en plus nécessaire de garantir la sécurité physique et informatique pour faire face aux attaques physiques, informatiques et hybrides.

Dans le présent rapport, le terme « sécurité » englobe la sécurité physique, la sûreté et la cybersécurité. Il doit être traité de manière globale et non fragmentée, car les infrastructures maritimes critiques (IC) comprennent à la fois des installations physiques et informatiques.

La sécurité physique et la cybersécurité sont des défis majeurs aux niveaux national et international. Les ports commerciaux sont des infrastructures critiques (IC) et des catalyseurs économiques clés. Leur sécurité est donc essentielle dans le secteur des activités maritimes. En outre, elle constitue l'un des plus grands avantages commerciaux dans l'ère numérique maritime internationale, qui est de plus en plus compétitive et en plein essor.

Les ports sont également des nœuds indispensables des chaînes d'approvisionnement puisqu'ils font intervenir de nombreuses activités, acteurs stratégiques et des partenaires commerciaux qui interagissent les uns avec les autres. La sécurité et la durabilité sont également devenues des sources de préoccupation importante dans les chaînes d'approvisionnement des ports. L'identification et la gestion des menaces, de leurs effets et des risques pour la chaîne d'approvisionnement constituent des défis majeurs. Les difficultés sont en partie dues à la complexité induite par le grand nombre d'activités, de processus, d'entités, et d'installations physiques et informatiques. En effet, tous ces éléments sont liés et interdépendants au sein de la chaîne d'approvisionnement. Les méthodologies et les outils de gestion des risques ciblés pour gérer les incidents de sécurité physique et informatique dans les ports et leurs chaînes d'approvisionnement représentent de véritables enjeux en matière de sécurité.

2 Un écosystème maritime complexe

Les ports commerciaux modernes, les compagnies maritimes et les navires dépendent fortement du fonctionnement de systèmes TIC complexes et dynamiques, et de chaînes d'approvisionnement maritimes basées sur les TIC. Les ports opèrent donc dans un environnement maritime complexe. L'environnement maritime (image 1) met en scène de nombreux acteurs et infrastructures (autorités, ports, compagnies maritimes et d'assurance, industrie navale, banques, chaînes d'approvisionnement, autres infrastructures critiques), ainsi que des installations (physiques et informatiques).

Image 1: Environnement maritime[1]

Les infrastructures maritimes sont considérées comme critiques au regard des directives NIS et NIS2 (directives sur la sécurité des réseaux et des systèmes d'information)[2], car l'interruption de leurs opérations et de leurs services aurait un impact négatif, d'une part, sur le commerce national, européen et international au sens large, et, d'autre part, sur les vies humaines.

En tant qu'infrastructures critiques, les infrastructures maritimes sont tenues de maintenir la sécurité (physique et informatique) de toutes leurs installations TIC hébergées et exploitées dans leurs IC, afin de fournir des services portuaires. Les TIC maritimes peuvent être considérées comme un système informatique physique comportant six couches :

1. Couche « infrastructure » (bâtiments, plateformes, portes, marinas, centres de données, terminaux, navires)

2. Couche « télécom » (réseaux, équipements de télécommunication, satellites, stations relais, stations tributaires) ;

[1] (Polemi, 2017)
[2] (Directive (UE) 2016/1148 du Parlement Européen et du Conseil 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, 2016); (Negreiro, 2022)

3. Couche « informatique » (systèmes de navigation / de transmission / de surveillance / communautaire portuaire, SIG, systèmes de surveillance intelligents, Internet des objets (IoT)) ;

4. Couche « données » (données maritimes et côtières, données commerciales) ;

5. Couche « services maritimes » (facturation, navigation, gestion des bagages, du fret, des navires et des conteneurs, logistique, services de la chaîne d'approvisionnement);

6. Couche « utilisateurs » : a. utilisateurs internes (opérateurs, administrateurs, équipage) ; b. utilisateurs externes (autorités portuaires, compagnies maritimes, douanes, compagnies d'assurance, fournisseurs de technologies de l'information et de la chaîne d'approvisionnement) ; et c. objets intelligents (conteneurs, navires, cargaison de l'équipage, bagages, véhicules).

La première (infrastructure) et la sixième (utilisateurs) sont les couches physiques des infrastructures maritimes critiques, tandis que les couches 2 à 5 sont liées à l'informatique. Les acteurs maritimes doivent garantir la confidentialité, l'intégrité et l'authenticité de l'ensemble des TIC, c'est-à-dire la sécurité des installations physiques (sûreté) et la sécurité des installations informatiques (cybersécurité).

Les infrastructures maritimes critiques revêtent une importance économique croissante et sont devenues une cible pour les pirates informatiques, qui lancent de plus en plus d'attaques physiques et informatiques contre les systèmes de navigation globale et les systèmes de gestion des cargaisons des ports et des navires. Ces attaques peuvent mettre un navire hors service, le détourner ou entraîner le vol de sa cargaison, tout en compromettant les données sensibles des clients ou des entreprises.

De même, les attaques visant les systèmes d'exploitation des terminaux (TOS), les systèmes communautaires portuaires (PCS) (par ex., les systèmes de contrôle de surveillance, les SCADA, les systèmes de contrôle distribués et les contrôleurs logiques programmables) ou les systèmes de navigation peuvent perturber ou endommager des dispositifs mécaniques essentiels (notamment les grues à conteneurs, les systèmes de sécurité et les systèmes mécaniques qui font fonctionner les écluses et les barrages). Pire encore, ces attaques peuvent causer des pertes humaines, entraîner le vol de cargaisons ou la destruction de navires. Une attaque sur un TOS de conteneurs pourrait également perturber les services de conteneurs intermodaux qui s'appuient sur le transport maritime, ferroviaire et routier.

Les anciens TOS portuaires ont une longue durée de vie et disposent souvent d'un mode de fonctionnement indépendant, c'est-à-dire avec une sécurité et des mots de passe inadéquates, sans mécanismes ni protocoles de protection des données. Ce mode de fonctionnement les rend vulnérables à l'espionnage, aux arrêts et à l'interception. Toutes ces failles peuvent entraîner la perturbation de divers services et opérations portuaires et des chaînes d'approvisionnement essentiels. Les PCS sont des plateformes électroniques complexes qui relient de multiples systèmes exploités par diverses organisations de

l'écosystème maritime et une pléthore de fournisseurs de TIC. La sécurité des PCS est traitée comme une « boîte noire » cryptographique, dans laquelle les rouages internes sont cachés et dont seules les entrées et sorties sont connues.[3] Les guichets uniques nationaux, qui reposent sur le PCS, doivent être évalués et les politiques de sécurité qui les accompagnent doivent garantir la fiabilité de leur fonctionnement.

Malheureusement, la plupart des acteurs maritimes se basent sur des pratiques de gestion de la sécurité non normalisées et non harmonisées. Elles se concentrent sur les menaces et les failles physiques et non pas sur celles d'origine informatique. Les incidents physiques et informatiques peuvent compromettre le fonctionnement des ports, des navires et de l'ensemble de la chaîne d'approvisionnement, entraînant ainsi des perturbations économiques, des dysfonctionnements des systèmes de transport et du commerce international. En outre, les chaînes d'approvisionnement touchées peuvent devenir une cible pour les terroristes internationaux si les ports et toutes les entités de la chaîne n'ont pas effectué des contrôles de sécurité appropriés.

Ce rapport sert de manuel de sensibilisation et de guide de bonnes pratiques. Il a pour tâche de détailler les principales questions relatives à la sécurité (sûreté et cybersécurité) de l'infrastructure d'information critique (IIC) maritime, mais également de décrire les menaces et les attaques informatiques auxquelles l'écosystème maritime (ports, navires, compagnies maritimes, chaînes d'approvisionnement maritimes) doit faire face en raison d'une numérisation rapide. Les conséquences et l'impact de ces menaces sur les opérateurs maritimes, les parties prenantes, les économies et la sécurité nationale peuvent être incommensurables. Les normes, stratégies et instruments juridiques et politiques en matière de cybersécurité sont présentés comme des exemples d'efforts à déployer pour relever de manière globale les défis liés à la cybersécurité maritime. Les méthodologies, outils et lignes directrices de gestion des risques basés sur les normes sont détaillées afin de sensibiliser les ports africains aux approches internationales existantes. Le respect des normes et des stratégies de sécurité existantes renforce la résilience et la collaboration, ce qui permet de sécuriser les opérations internationales, les chaînes d'approvisionnement et le commerce. Enfin, les auteurs ont formulé des recommandations à l'attention des ports africains et proposé des questionnaires pour évaluer la maturité des ports en matière de cybersécurité.

[3] (Acharya, 2019)

3 L'Union européenne (UE) et les ports africains

3.1 Introduction

Définitions clés :

Installation portuaire : un emplacement où a lieu l'interface navire/port ; elle comprend des zones telles que les zones de mouillage, les postes d'attente et leurs abords à partir de la mer, selon le cas [règlement (CE) n° 725/2004].

Port : toute étendue déterminée de terre et d'eau, dont le périmètre est défini par les États membres dans lequel le port est situé, comprenant des infrastructures et équipements destinés à faciliter les opérations de transport maritime commercial [directive 2005/65/CE].

Les *IC portuaires* comprennent les installations portuaires (installations physiques des ports), les installations informatiques et les utilisateurs. Selon Alderton (1999), il existe trois types classiques de propriété et d'exploitation portuaire: Port propriétaire, Port outil et Port service.

Responsabilités de l'autorité portuaire (Source : Alderton, 1999)[4]			
Type de port	Infrastructure	Superstructure	Chargement, déchargement et arrimage
Port propriétaire	Oui	Non	Non
Port outil	Oui	Oui	Non
Port service	Oui	Oui	Oui

Le *port propriétaire* est celui où l'État, l'autorité portuaire ou le conseil municipal possède le terrain et loue le terminal à des manutentionnaires privés. L'État fournit les infrastructures telles que les quais et les terrains pour le terminal, tandis que l'opérateur privé fournit la superstructure et les équipements tels que les grues, l'entrepôt, l'équipement du terminal et d'autres installations commerciales. L'autorité portuaire de Rotterdam, qui loue l'infrastructure portuaire à European Combined Terminal (ECT), en est un exemple.

Le *port outil* représente une situation dans laquelle l'État possède à la fois l'infrastructure et la superstructure, et l'entreprise privée de manutention fournit la main-d'œuvre nécessaire à l'exploitation. La concurrence est très forte et les appels d'offres sont soumis à des droits bien encadrés. C'est le cas de Houston aux États-Unis et de la plupart des ports autonomes en France.

Le *port service* est également appelé « port global » ou « port public ». L'État ou l'autorité portuaire est propriétaire de l'infrastructure et de la superstructure. Il/elle fournit tous les services et installations pour les navires. L'autorité portuaire de Singapour, qui a été privatisée en 1997, et les ports d'Inde, d'Israël, d'Afrique du Sud et du Ghana en sont des exemples.

La *couche physique des ports* comprend les quais, les pontons, les canaux d'accès, etc. En général, les conditions à l'intérieur d'un port varient d'un terminal à l'autre. Cependant, tous

[4] (Alderton, 1999)

les ports doivent relever le défi de maintenir leur infrastructure dans des environnements maritimes difficiles.

Superstructure portuaire : il s'agit des aménagements de surface (par ex. pour le stockage), des équipements fixes (tels que les entrepôts et les terminaux), ainsi que des équipements mobiles (comme les grues) situés dans un port visant à fournir des services liés au transport.

Manutention portuaire : Ce concept comprend le chargement, le déchargement et l'arrimage de la cargaison sous toutes ses formes à bord des navires dans les ports.

Chaque entité ayant des responsabilités au sein de l'autorité portuaire doit identifier ses installations critiques dans son domaine de responsabilité et évaluer en conséquence le niveau de risque.

Presque toutes les installations sont liées au cyberespace de trois manières, à savoir : 1) le site technologique et les systèmes d'information et de communication (matériel/logiciel) ; 2) les procédures d'exploitation des systèmes TIC ; et 3) les personnes et les objets intelligents (par ex., l'IoT) qui interagissent avec les systèmes TIC.

3.1.1 Les ports africains

Les exportations africaines de biens et de services ont connu leur croissance la plus rapide au cours de la dernière décennie, mais les volumes africains restent faibles puisqu'ils ne représentent que 3 % du commerce international, selon la Banque mondiale[5]. Le rôle limité de l'Afrique dans le commerce mondial se reflète dans les contours de ses ports maritimes, qui doivent faire face à des défis grandissant en matière de sûreté, de sécurité et de cybersécurité. Néanmoins, les ports maritimes constituent un élément essentiel de la chaîne d'approvisionnement en Afrique. En effet, le transport maritime représente la principale porte d'accès au marché mondial et chaque port permet de faire le lien avec la partie intérieure du pays en question. Cet accès intérieur s'étend souvent sur plusieurs pays enclavés, lesquels représentent un tiers de l'Afrique. Il est donc essentiel d'investir et de moderniser les ports et les infrastructures de transport connexes pour faire progresser l'économie nationale et promouvoir le développement et la croissance économiques de l'Afrique.

Une étude de PricewaterhouseCoopers (PWC)[6] montre que les volumes économiques traités dans les principaux ports d'Afrique subsaharienne le sont principalement dans des ports basés en Afrique de l'Ouest et dans le Golfe de Guinée (voir l'image ci-dessous).

[5] (Greater and More Diverse Participation in Global Trade is Key to Achieving Africa's Economic Transformation, says New World Bank Book, 2022)
[6] (Strenghtening Africa's gateways to trade, 2018)

Image 2: Ports africains[7]

Les pays du Golfe de Guinée dépendent de mers protégées et sûres pour leur développement économique, le libre-échange, le transport maritime et la préservation de l'environnement marin. Il s'agit d'une vaste région maritime qui couvre 18 pays, compte 500 millions d'habitants et s'étend du Sénégal à l'Angola, avec plus de 5 700 km de côtes. La région est une route maritime internationale importante et représente 25 % du trafic maritime africain. Le pétrole et le poisson, parmi divers types de ressources naturelles, sont des marchandises importantes transportées vers différents pays africains, mais aussi vers l'Europe et d'autres pays du monde par des navires commerciaux.

Les ports maritimes représentent l'interface entre la haute mer et l'arrière-pays. Ils constituent des infrastructures maritimes d'importance stratégique par lesquelles tous les biens économiques doivent transiter. Cette situation les rend très vulnérables puisqu'ils deviennent la cible d'organisations criminelles et/ou de groupes terroristes. Les attaques terroristes contre les ports pourraient avoir de graves répercussions sur les populations locales, les infrastructures portuaires elles-mêmes, et les économies locales et régionales qui dépendent de ces activités.

Même si sa part dans les échanges a diminué, l'UE reste le principal partenaire commercial de l'Afrique. Entre temps, les échanges commerciaux avec la Chine ont augmenté. Sur le continent africain, l'Afrique de l'Ouest est le premier partenaire commercial de l'UE en Afrique subsaharienne. L'Europe importe d'Afrique de l'Ouest des produits finis (poissons et textiles), mais aussi des produits bruts tels que des combustibles et des produits agricoles alimentaires. L'Afrique de l'Ouest, quant à elle, importe de l'UE des carburants raffinés, des produits alimentaires, des machines, des produits chimiques et pharmaceutiques. Selon la CNUCED, l'Afrique de l'Ouest est également la principale destination des investissements de l'UE en Afrique.[8]

[7] (*Strengthening Africa's Gateway to Trade*, 2018)
[8] (Maritime trade and Africa, 2018)

Il appartient à chaque pays de déterminer si sa législation nationale en matière de sécurité et le code international pour la sûreté des navires et des installations portuaires (ISPS) de l'Organisation maritime internationale (OMI) sont correctement gérés et mis en œuvre. Il est possible d'accompagner les ports dans une perspective plus large afin d'accroître leur résilience en matière de sécurité. Cette étude doit servir de recueil de recommandations dont l'objectif est d'améliorer la sécurité des ports en Afrique subsaharienne.

3.1.2 Commerce maritime entre l'UE et l'Afrique

Le caractère critique du secteur maritime pour les États communautaires et leurs économies est clairement illustré par le fait qu'il existe 329 ports commerciaux européens par lesquels transitent 74 % de marchandises importées et exportées et 37 % des échanges au sein de l'Union.

L'UE et les États-Unis sont les principaux partenaires commerciaux du continent africain.[9] Le programme d'investissement « Global Gateway » Afrique – Europe[10] a pour objectif de soutenir l'Afrique à :

- Accélérer la transition écologique
- Accélérer la transition numérique
- Accélérer la croissance durable et la création d'emplois décents
- Renforcer les systèmes de santé
- Améliorer l'éducation et la formation

Le Centre africain de coopération de technologie maritime (MTCC) a été lancé à Mombasa en 2017. Il fait partie du réseau mondial MTCC (GMN) financé par l'Union européenne[11]. Le MTCC pour l'Afrique (MTCC Afrique) est hébergé par l'Université Jomo Kenyatta d'agriculture et de technologie (JKUAT), campus CBD de Mombasa, en partenariat avec l'Autorité maritime du Kenya (KMA) et l'Autorité portuaire du Kenya (KPA).

Le MTCC Afrique se concentre sur les points suivants :

- Faciliter le respect de la convention internationale pour la prévention de la pollution par les navires (annexe VI de la convention MARPOL) ;
- Améliorer les capacités de la région en travaillant avec les administrations maritimes, les autorités portuaires, les ministères et les acteurs du secteur du transport maritime en vue de faciliter le respect des réglementations internationales en matière d'efficacité énergétique des navires ;
- Promouvoir l'adoption de technologies et d'opérations à faible émission de carbone dans le secteur maritime par le biais de projets pilotes ;
- Sensibiliser aux politiques, stratégies et mesures visant à réduire les émissions de gaz à effet de serre et les autres émissions du secteur du transport maritime ;
- Faire la démonstration d'un système pilote de collecte de données et d'établissement de rapports sur la consommation de carburant des navires afin d'améliorer la compréhension des armateurs et des administrations maritimes ;

[9] (Coulibaly, Kassa, & Zeufack, 2022)
[10] (EU-Africa: Global Gateway Investment Package, n.d.)
[11] (Africa Maritime Technology Cooperation Centre launched in Mombasa, 2017); (MTCC Africa, n.d.)

- Diffuser et partager les résultats et les expériences du projet par des actions de communication et de visibilité appropriées ; et
- Élaborer et mettre en œuvre des stratégies visant à maintenir l'impact des résultats et des activités du MTCC au-delà de la durée du projet.

La revue mensuelle « Eurostatistics » mentionnait en 2021 que le plus grand partenaire commercial de l'Afrique était l'Europe, avec 33 % de ses exportations vers l'Europe et 31 % de ses importations en provenance de l'Europe. Cela équivaut à des importations d'une valeur de 142 milliards d'euros et à des exportations de 146 milliards d'euros de marchandises en provenance ou à destination de l'Afrique en 2021.

L'Afrique dépend fortement des navires et des ports pour assurer son commerce intercontinental, tandis que le tiers des pays enclavés reçoivent leurs marchandises par l'intermédiaire de pays disposant d'un accès à la mer. Le transport maritime reste donc la principale voie d'accès vers l'Europe.

Le commerce maritime africain se démarque par le fait que les activités commerciales internationales du continent se concentrent dans les ports maritimes. La CNUCED indique que les ports africains ne représentent que 4 % du volume mondial des échanges par conteneurs, dont les importations de produits manufacturés représentent une grande partie. Les ports africains ne sont pas alignés sur les tendances mondiales en matière de taux de conteneurisation maritime. Ils pourraient améliorer leurs volumes de trafic portuaire conteneurisé et augmenter les exportations de marchandises. Si plus de marchandises étaient acheminées par route depuis l'arrière-pays vers les ports, davantage de navires porte-conteneurs transiteraient par ces derniers. Cela permettrait d'attirer un trafic international plus important.

Pour y parvenir, il est nécessaire que les ports africains et les réseaux de transport terrestre modernisent leurs infrastructures et leurs services portuaires, et améliorent leurs performances et leurs niveaux de productivité. Il convient également de renforcer les initiatives en matière de sécurité, de cybersécurité et de sûreté portuaire au titre du code ISPS.

4 Concepts de sécurité maritime

4.1 Introduction

Dans notre monde soucieux de la sécurité, il est difficile de se souvenir d'une époque où la sécurité n'était pas une priorité. Aujourd'hui, les actions en matière de sécurité maritime s'améliorent chaque année dans diverses régions du monde, avec pour résultat une diminution progressive des accidents, des blessures, des attaques physiques et des cyberattaques. Mais ce type de protection n'a pas toujours été une priorité pour les armateurs et les ports maritimes. Les accidents et les cyberattaques survenus à bord des navires, dans les ports maritimes et dans les compagnies maritimes ont stimulé le passage d'une logique de réparation à une logique de prévention. Le dénominateur commun de ces incidents est que les règles de sécurité (sûreté et cybersécurité) existantes n'ont pas été suivies de près et n'ont pas été correctement mises en œuvre dans la pratique.

4.2 Concepts et terminologie de la sécurité

La littérature internationale utilise indifféremment les termes de sécurité, sûreté, cybersécurité, sécurité physique et résilience.

Dans le présent rapport, comme indiqué plus haut, les infrastructures maritimes critiques sont considérées comme des systèmes physiques et informatiques comportant des couches correspondantes. Les acteurs du secteur maritime doivent assurer la sécurité des installations physiques (sûreté) et la sécurité des installations informatiques à l'intérieur des couches (cybersécurité). L'objectif de la sécurité maritime est de protéger les installations matérielles (navires, bâtiments, marinas, centres de données, cargaisons, etc.) et les individus (personnel, opérateurs, équipage, etc.) contre divers types de menaces physiques. C'est-à-dire les incidents, les dangers, les préjudices intentionnels et non intentionnels tels que les catastrophes physiques, les tempêtes en mer, les incendies, le terrorisme, les troubles sociaux, la contrebande d'armes et de stupéfiants et la piraterie. L'objectif de la cybersécurité maritime est de préserver la confidentialité, l'intégrité et la disponibilité de toutes les installations informatiques (les télécommunications, les TIC, les données, les services) en cas de cybermenaces (notamment le phishing, le spoofing, l'ingénierie sociale, à savoir les activités malveillantes utilisant les interactions humaines, rusurpation d'identité, les accès non autorisés, les attaques par déni de service distribué (DDoS)).

La sécurité englobe la sûreté et la cybersécurité, comme l'illustre l'image 3**.**

Image 3: La sécurité englobe la sûreté et la cybersécurité

Les installations physiques et informatiques peuvent être exposées à des menaces si des contrôles/actions et des mesures d'atténuation appropriés n'ont pas été mis en œuvre. En effet, celles-ci seront plus vulnérables aux menaces et à l'exploitation. En cas d'incident de sécurité malheureux, des procédures de sécurité d'urgence, des plans de poursuite des activités et de reprise après sinistre sont activés, et des mesures sont prises pour atténuer les risques. Chaque fois qu'un incident se produit, une série de mesures sont déclenchées au niveau national, conformément aux plans d'urgence à bord du navire (plans de sûreté du navire), dans le port maritime (plan de sûreté du port) et dans les installations portuaires (plans de sûreté de l'installation portuaire).

Le bouclier de protection est le tronc commun qui lie la sûreté et la cybersécurité. Ce dernier s'applique dans chaque domaine. La mise en place de ce niveau de protection se fait par une gouvernance efficace, dont l'objectif est d'éliminer les risques physiques et informatiques, d'éviter les incidents de sécurité portuaire et de prévenir les accidents pouvant toucher des individus. L'une a un impact sur l'autre. Par exemple, si une cyberattaque dans une installation portuaire de marchandises diverses arrête soudainement les opérations de manutention par grue, la cargaison pourrait tomber dans la cale du navire et causer des blessures mortelles aux dockers qui se trouvent en dessous. C'est pourquoi cette étude aborde la **sécurité comme une combinaison entre la sûreté et la cybersécurité**. Elle présente la manière dont les réglementations, les normes et les meilleures pratiques peuvent être combinées pour traiter les deux composantes de la sécurité**.**

4.3 Technologies maritimes physiques et informatiques

Les ports et les navires abritent des infrastructures d'information critiques complexes avec des installations physiques et informatiques utilisées pour mener à bien leurs opérations et fournir leurs services.

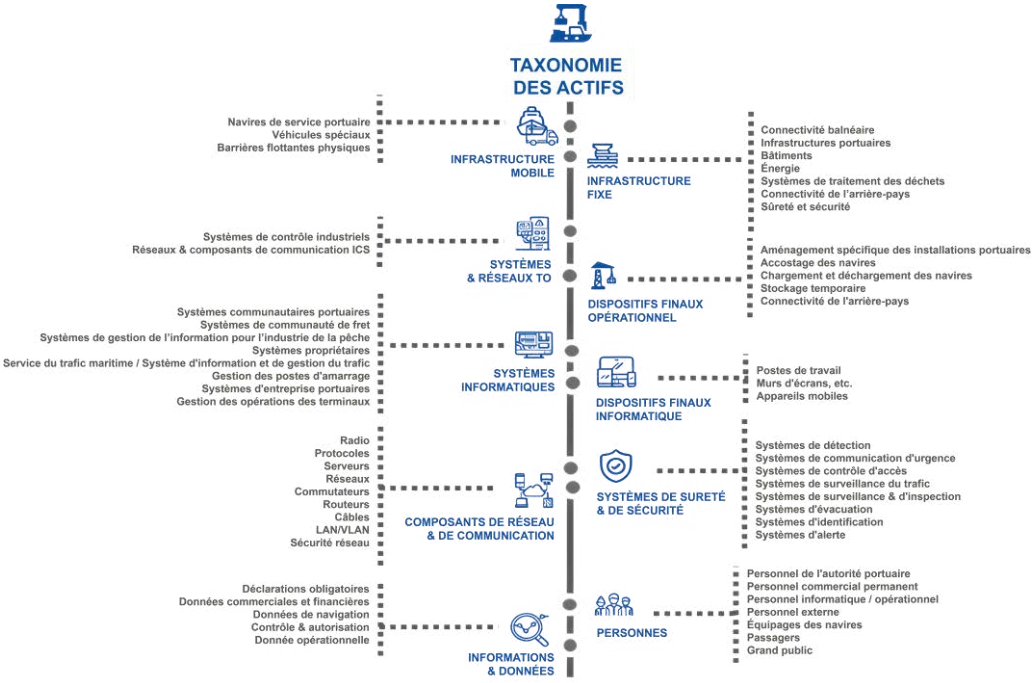


Image 4: Taxonomie des installations des ports maritimes élaborée par l'ENISA[12]

[12] (Drougkas, Sarri, Kyranoudi, & Zisi, 2019)

Les navires sont dotés de diverses technologies, notamment : des systèmes de positionnement, un système de visualisation des cartes électroniques et d'information (ECDIS), des systèmes de contrôle et de surveillance des moteurs, un système mondial de détresse et de sécurité en mer (SMDSM), un système d'identification automatique (AIS) et un système de supervision industrielle maritime (SCADA). L'image suivante illustre les technologies embarquées :

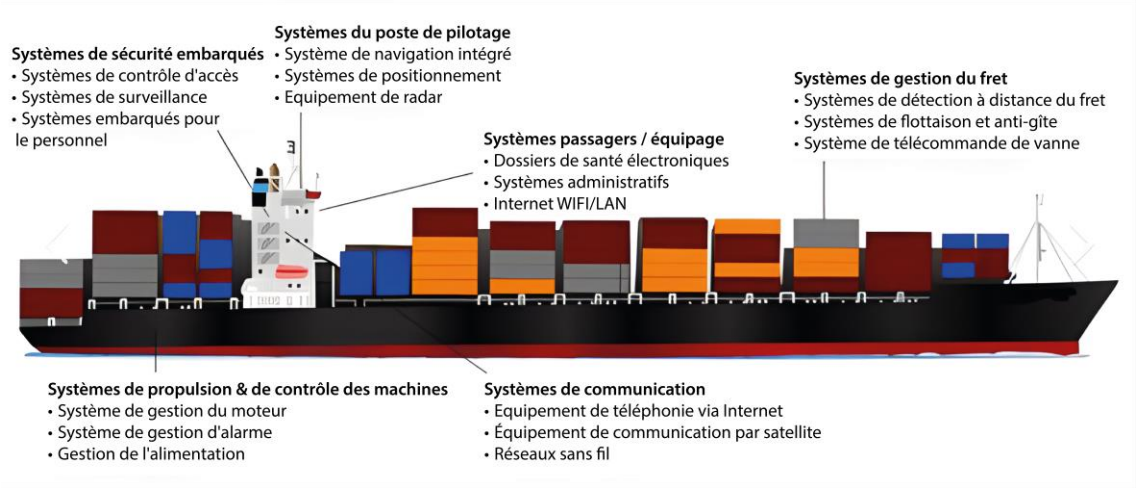


Image 5 : Technologies navales[13]

Les technologies portuaires et navales sont utilisées pour fournir des services portuaires et des services liés à la chaîne d'approvisionnement maritime. En voici quelques exemples :

- Services d'accostage des navires
- Services de chargement et de déchargement des navires
- Services de stockage temporaire et d'hébergement
- Services de distribution et de transfert
- Services d'appui
- Services des autorités
- Services de sécurité
- Transport de marchandises (par ex., gaz naturel liquéfié (GNL), véhicules, céréales)
- Services de croisière et transport de personnes
- Services de gestion des conteneurs
- Services de transport maritime côtier

[13] Source : https://www.hvassallo.com/practice-areas/maritime-cyber-security/; consulté le 17 décembre 2022

Image 6: Technologies portuaires[14]

4.3.1 Numérisation accélérée du secteur maritime

Les technologies émergentes, telles que l'intelligence artificielle (IA), la 5G, le Big Data, l'IoT, la robotique et les technologies satellitaires sont adoptées dans le cadre de nouvelles avancées maritimes, comme les navires autonomes et l'inspection rapide des IC portuaires. Parmi ces IC on retrouve les parcs éoliens, les stations benthiques, l'automatisation des opérations de levés géophysiques, géotechniques et sismiques, la surveillance et la gestion des navires.

L'adoption accélérée des technologies numériques dans l'écosystème maritime conduira à de nombreuses innovations dans diverses fonctions maritimes, comme l'échange de quantités massives d'informations à l'aide de réseaux de communication acoustiques et optiques avancés, l'automatisation des décisions collectives, le partage de ressources complémentaires, l'automatisation de la maintenance et de l'exploitation des ports et des navires. Toutefois, ces innovations à venir s'accompagneront de nouvelles menaces physiques et informatiques. Une gouvernance de la sécurité (sûreté et cybersécurité) sera nécessaire pour s'assurer que les autorités portuaires, les armateurs et toutes les parties prenantes du secteur maritime disposent de la structure, des outils et des connaissances nécessaires pour maximiser les performances de leurs infrastructures en matière de sécurité (dans les ports et à bord des navires), et atteindre leurs objectifs conformément à la législation en matière de sécurité maritime et aux meilleures pratiques internationales.

4.4 Incidents de sécurité et acteurs de la menace

Chaque port doit développer une gouvernance de travail sur mesure avec des pratiques efficaces de gestion des risques (physiques et informatiques) qui garantissent la sécurité des infrastructures critiques, des opérations et des services maritimes.

4.4.1 Types d'attaquants

Les *cybercriminels* sont des adversaires qui commettent une action illégale en utilisant des moyens numériques. Si l'objectif de l'attaque est illégal (par ex., vol, délit grave, vandalisme,

[14] Source : (Burt, 2021)

terrorisme), l'auteur est alors qualifié de cybercriminel. Les adversaires sont classés en fonction de leurs motivations, de leurs capacités et des possibilités qui s'offrent à eux :

- *Acteurs intentionnels* : les auteurs d'attaques internes font partie d'une certaine catégorie de menaces. Ils possèdent une connaissance détaillée d'une organisation et de ses systèmes.
- *Cyberterroristes :* ils mènent des activités violentes pour influencer l'opinion publique et le processus de prise de décision.
- *Hacktivistes / activistes civils* : ils mènent des attaques pour des raisons idéologiques dans le but d'attirer l'attention sur un programme politique, social, religieux ou moral.
- *Cybercriminels (organisés) :* leur objectif est d'obtenir un profit financier, d'influencer des élections, d'abuser des individus. Toutes les activités criminelles traditionnelles menées à l'aide de moyens numériques appartiennent à cette catégorie.
- *Script Kiddies :* Il s'agit de jeunes acteurs ayant peu de connaissances et de capacités, dont le but est habituellement de s'amuser, de remporter un pari ou un prix.
- *Les attaquants parrainés par un État ou les espions gouvernementaux* agissent pour obtenir un accès à des informations privilégiées, telles que la propriété intellectuelle, les projets commerciaux, les feuilles de route, les données relatives au personnel ou aux clients, mais également pour avoir un aperçu des opérations commerciales et des décisions à venir.
- *Les concurrents / espions industriels* tentent d'obtenir un avantage commercial en volant la propriété intellectuelle, la documentation sur les opérations et les décisions de l'entreprise ou les données des clients.
- *Les cyberguerriers recrutés par un gouvernement et les cybercombattants individuels* sont des acteurs motivés par le patriotisme. Ils sont soit directement contrôlés par un État soit constitués d'individus ou de groupes de personnes motivés par des valeurs politiques, sociales, ethniques ou religieuses communes.
- La principale motivation *des cyber-vandales et des cyber-punks* est la destruction de biens. Ils sont stimulés par la recherche de la satisfaction personnelle et de la domination.
- *Les hackers « black hat », ou « Crackers »* tentent de pénétrer les systèmes par curiosité et par intérêt personnel. Ils peuvent obtenir des récompenses financières provenant de l'exploitation de données, de produits et de systèmes obtenus, ou gagner en réputation et reconnaissance parmi leurs pairs.

Il existe également des *acteurs involontaires*, qui sont généralement des employés non formés ou imprudents, mais qui peuvent tout de même porter préjudice à l'organisation. Ils n'ont pas d'intentions malveillantes mais sont mentionnés dans cette étude, car leurs actions peuvent représenter un risque pour la sécurité.

4.4.2 Incidents de sécurité

Les opérations portuaires et maritimes dépendent de plus en plus de l'efficacité des systèmes basés sur des logiciels. Les navires et les ports qui peuvent tirer parti des nouvelles technologies et des solutions numériques seront mieux lotis que les autres. Par exemple, la communication entre les navires et les opérations de manutention portuaire nécessitent le transfert d'informations par le biais d'ordinateurs. Ces systèmes de technologie de

l'information (TI) gèrent toutes les tâches administratives liées à la préparation, à l'exécution et au traitement du fret. Les machines de manutention des terminaux, telles que les grues à conteneurs et les machines à bord des navires disposent de connexions numériques avec d'autres systèmes de commande à distance. Ces machines mécaniques dotées d'un équipement numérique sont appelées systèmes de technologie opérationnelle (TO). On peut généralement dire que les systèmes TO contrôlent le monde physique, comme les machines, tandis que les systèmes TI gèrent les données et les informations. Un système TI gère le flux d'informations numériques (données), alors qu'un système TO gère le fonctionnement des processus physiques et les machines utilisées pour les exécuter. Dans le monde maritime, « TO » désigne le matériel, les systèmes et les logiciels des navires et des ports qui font fonctionner les navires et les équipements de manutention portuaire. Ils surveillent et contrôlent les dispositifs physiques ainsi que les processus. Le terme « TI » désigne les ordinateurs et les serveurs utilisés dans les bureaux pour gérer le traitement de l'information, notamment les logiciels, le matériel et les technologies de communication.

Ces systèmes TO et TI ne sont pas toujours bien protégés contre les cyberattaques. Les risques liés aux systèmes TI affectent principalement les finances et la réputation, tandis que ceux liés aux systèmes TO peuvent toucher et menacer l'infrastructure portuaire, voire coûter des vies. Les ports maritimes et les navires peuvent sembler être des cibles inhabituelles pour les cyberattaques, mais ces dernières visent de plus en plus les opérateurs maritimes et des attaques réussies sont régulièrement signalées dans le monde entier. C'est pourquoi la sécurité informatique devient de plus en plus importante pour résister aux cyberattaques dans le secteur maritime.

Pendant longtemps, la direction générale des ports et des compagnies maritimes a considéré la cybersécurité et la gestion des risques comme une tâche relevant du service informatique. Néanmoins, cette situation est en train de changer rapidement, car l'ensemble du personnel est impliqué dans la gestion et l'atténuation des risques informatiques.

L'impact d'une cyberattaque peut se propager aux installations matérielles. A titre d'exemple, une cyberattaque peut désactiver le système intelligent de détection des incendies et les systèmes d'extinction automatique d'un méthanier dans un grand port d'Afrique, et déclencher ainsi un incendie. Les cyberattaques et tout type d'incident de sécurité/sûreté peuvent avoir un impact négatif sur les chaînes d'approvisionnement maritimes ainsi que sur le commerce local et international. Par exemple, une cyberattaque sur le système de navigation électronique peut désorienter un navire, le faire entrer en collision et couler à l'entrée d'un grand port de l'UE ou d'Afrique. L'enlèvement de l'épave et la remise en service du port peuvent prendre plusieurs semaines, sans compter les dommages économiques, juridiques et commerciaux subis par les chaînes d'approvisionnement africaines et européennes en raison de l'interruption des échanges.

Les navires peuvent être utilisés comme moyen de transport pour les terroristes ou pour introduire clandestinement des armes dans un pays. Ils peuvent également être utilisés pour faire exploser une bombe à bord du navire afin de faire sauter une partie critique du port.

Malheureusement, une enquête de 2018 sur la cybersécurité[15] a révélé que peu d'entreprises de transport maritime étaient en mesure de faire face à une cyberattaque sans subir trop de dégâts. Il est évident que le secteur a plus que jamais besoin de lignes directrices et de législations pertinentes à cet égard. Il est nécessaire que les ports mettent en œuvre un plan de gouvernance efficace qui tienne compte des procédures et processus de gouvernance physique et de cybersécurité.

4.4.2.1 Accidents de sécurité

Plusieurs accidents maritimes et catastrophes navales mortelles sont considérés comme des incidents de sécurité. Prenons l'exemple du naufrage du RMS Titanic en avril 1912. Le Titanic a été l'un des premiers bateaux à passagers à sombrer, entraînant la perte de plus de 1 500 vies. Cette catastrophe et le grand nombre de victimes sont dus à une navigation imprudente à proximité d'icebergs et à un nombre insuffisant de canots de sauvetage pour secourir toutes les personnes à bord.[16] Autre exemple : le naufrage du ferry M/S Estonia en 1994. La proue du pont de chargement n'était pas fermée de manière étanche et s'est ouverte lors d'une tempête, entraînant le naufrage du navire et la perte de plus de 850 passagers.[17] Un accident similaire s'est produit avec le Ferry Herald of Free Enterprise en 1987, causant la perte de 197 personnes et de l'ensemble du navire avec sa cargaison.[18] En 2004, le navire-citerne M/V Bow Mariner, chargé d'éthanol, a explosé, coulé et emporté avec lui 21 membres d'équipage dans une tombe marine. La raison de cette catastrophe[19] est la violation de plusieurs règles de sécurité, qui a provoqué l'explosion du navire et alourdi le bilan humain. Un accident plus récent : la catastrophe du Costa Concordia en 2012. Le capitaine a navigué trop près des rochers, ce qui a entraîné la perte du navire et coûté la vie à 32 personnes.[20]

Dans les ports maritimes, de nombreux accidents peuvent se produire lors d'opérations de déchargement et de chargement des navires, mais aussi dans les terminaux et la zone portuaire commune. Une étude réalisée par R. Darbra et J. Casal[21] sur des centaines d'accidents survenus dans les ports maritimes a conclu que les accidents les plus fréquents étaient les rejets de gaz (51 %), suivis par les incendies (29 %) et les explosions (17 %). Plus de la moitié des accidents se sont produits lors d'opérations de chargement et de déchargement, mais les accidents dans les entrepôts de stockage, les usines chimiques et les opérations à l'intérieur de la zone portuaire ont également contribué de manière significative au nombre total d'accidents. Parmi les accidents récents graves, on peut citer celui qui s'est produit dans le port de Beyrouth en août 2020, où une explosion a dévasté plusieurs parties de la ville. L'enquête a révélé que l'accident a été provoqué par l'explosion de 2 750 tonnes de nitrate d'ammonium qui avaient été stockées dans le port de Beyrouth après la saisie d'un navire.[22]

[15] (Jørgensen, 2018)
[16] (Titanic, n.d.)
[17] (Langewiesche, 2004)
[18] (Herald of Free Enterprise Ferry Disaster – 1987, n.d.)
[19] (Shapira, 2006)
[20] (Costa Concordia: What happened, 2015)
[21] (Darbra & Casal, 2004)
[22] (The Beirut Port Explosion, n.d.)

4.4.2.2 Cyberattaques

Les cyberattaques contre les infrastructures maritimes peuvent être variées. Afin d'attirer l'attention des lecteurs sur les menaces potentielles de tels actes malveillants et d'analyser plus en détail les mécanismes de ces attaques, voici quelques exemples de cyberattaques récentes :

- Le 10 avril 2020, la Mediterranean Shipping Company (MSC) a été la cible d'une attaque par logiciel malveillant.[23] Pour des raisons de sécurité, les serveurs de la MSC ont été fermés afin de protéger les données de l'entreprise et le site web de la compagnie a été mis hors ligne. L'attaque a perturbé les processus de données internes.
- Le 8 juillet 2019, une attaque par logiciel malveillant a ciblé un navire en partance pour le port de New York, engendrant la perte de données critiques. Les garde-côtes ont indiqué que l'absence de stratégies de sécurité sur le navire était la principale raison pour laquelle le navire avait été ciblé par cette attaque.[24] Tous les membres de l'équipage du navire partageaient le même identifiant et le même mot de passe pour accéder à l'ordinateur du navire. En outre, le pirate a profité de l'utilisation d'appareils externes et de l'absence d'antivirus.
- En mars 2019, une attaque par ransomware (demande de rançon) a complètement paralysé le réseau mondial de la compagnie maritime Norsk Hydro, victime du logiciel malveillant « LockerGoga ». Norsk Hydro a estimé que les pirates avaient pu pénétrer son réseau pendant deux à trois semaines avant d'être découverts. Plus de 22 000 ordinateurs et des milliers de serveurs dans cinq pays ont été touchés. « LockerGoga » a interrompu la production et les activités administratives de la compagnie pendant plusieurs jours. Les dégâts sont estimés à 71 millions de dollars.[25]
- En 2018, le gouvernement chinois a été soupçonné d'avoir mené une attaque par ransomware sur un sous-traitant de la marine américaine et subtilisé des données de sécurité très sensibles, notamment des plans pour un projet de missile supersonique.[26]
- En septembre 2018, des cyberattaques ont touché les ports de Barcelone (Espagne) et de San Diego (États-Unis). L'attaque par ransomware du port de San Diego s'est avérée être une infection par le logiciel malveillant « SamSam ».[27] L'impact a été limité à certaines fonctions administratives de l'autorité portuaire et n'a pas interrompu ses opérations ou les mouvements de navires. Le port de Barcelone n'a pas immédiatement divulgué le type d'incident, mais a indiqué que l'attaque avait perturbé ses systèmes informatiques internes, sans toutefois affecter les opérations des navires ou du port.
- En juillet 2018, la China Ocean Shipping Company (COSCO) a elle aussi été victime du ransomware « SamSam ». Lors de son attaque, le logiciel malveillant a perturbé les réseaux de la COSCO aux États-Unis, au Canada, au Panama, en Argentine, au Brésil,

[23] (Hand, 2020)
[24] (Winder, 2019)
[25] (Tomter & Gundersen, 2019)
[26] (China hackers steal data from US Navy contractor - reports, 2018)
[27] (Port of San Diego: phishing emails remain amongst greatest cyber threats, 2021)

au Pérou, au Chili et en Uruguay. Il aura fallu cinq jours à l'entreprise pour rendre de nouveau son système opérationnel.

- Le groupe A.P. Moller-Maersk a été touché par une attaque dévastatrice en juin 2017 à cause du logiciel malveillant « NotPetya ».[28] Maersk a dû interrompre ses activités pendant dix jours pour se remettre de l'attaque. Le groupe a dû réinstaller 4 000 serveurs, 45 000 PC et 2 500 applications. Maersk aurait perdu environ 300 millions de dollars de revenus.

Le tableau ci-dessous présente les principales cybermenaces pour 2022 selon le rapport « Gestion des risques informatiques dans les ports » de l'Agence européenne pour la cybersécurité (ENISA).

Cybermenace	Incident informatique			Référence :
	Organisation touchée :	Date :	Impact :	
Logiciels malveillants/ Ransomware	Systèmes informatiques	2022	Principaux terminaux pétroliers en Europe	https://www.france24.com/en/live-news/20220203-european-oil-port-terminals-hit-by-cyberattack
Logiciels malveillants/ Ransomware	Compagnies pétrolières	2022	Port d'Anvers	https://www.dw.com/en/belgium-investigates-cyberattack-on-energy-companies/a-60651892
Logiciels malveillants	Systèmes informatiques	2021	Oil tanking Deutschland GmbH & Co. KG	https://www.bbc.com/news/technology-60215252
Logiciels malveillants/ Ransomware (Mailto)	Toll Group	2020	Destruction de données	https://www.itnews.com.au/news/toll-group-hit-by-new-variant-of-mailto-ransomware-537537
Logiciels malveillants	Mediterranean Shipping Company (MSC)	2020	Panne de réseau	https://www.wsj.com/articles/mediterranean-shipping-co-hit-by-network-outage-considering-potential-cyberattack-11586523861
Logiciels malveillants	CMA CGM	2020	Brèche de sécurité	https://www.reuters.com/article/uk-cma-cgm-cyber-idUKKBN26L2N0
Logiciels malveillants/ Ransomware	Services administratifs du port	2018	Ports de San Diego et Barcelone	https://www.acronis.com/en-us/blog/posts/ransomware-attacks-sail-san-diego-and-barcelona/
Logiciels malveillants/ Ransomware	COSCO	2018	Panne du réseau local	https://www.forbes.com/sites/leemathews/2018/07/26/another-shipping-giant-falls-victim-to-ransomware/?sh=6aa75bd70d04
Logiciels malveillants/ Ransomware (NotPetya)	A.P. Moller-Maersk	2018	Destruction de données	https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

[28] (Greenberg, 2018)

Violation de données	Le service du port contrôlant le mouvement et la localisation des conteneurs.	2013	Port d'Anvers	https://www.bbc.com/news/world-europe-24539417

Les changements géopolitiques ont également un impact sur la sécurité des opérations maritimes. Au cours de la guerre en Ukraine en 2022, les navires transitant par la mer Noire et la mer d'Azov ont subi une série de cyberattaques. L'administration maritime américaine (MARAD) a indiqué que les navires avaient été victimes d'interférences GPS, d'usurpation d'identité AIS et de brouillage des communications. Le centre de transport maritime de l'OTAN et l'administration maritime américaine ont signalé des attaques par DDoS sur ces navires.

4.4.2.3 Attaques TI/TO

De nombreux navires utilisent encore des systèmes d'information et des technologies TI/TO qui ne sont pas conçus pour résister aux cyberattaques. S'ils ne sont pas correctement protégés, les pirates informatiques peuvent exploiter leurs vulnérabilités. Si les pirates peuvent contrôler le système du navire à distance, ils peuvent prendre le contrôle des systèmes d'information et de communication. Un navire est un système de systèmes intégré. C'est la raison pour laquelle les systèmes d'infrastructures d'information critiques d'un navire doivent être définis et évalués, leur sécurité contrôlée en permanence et inspectée régulièrement. Les pirates informatiques peuvent également se livrer à d'autres activités :

- usurper les systèmes de navigation
- contrôler le pilote automatique du navire
- brouiller ou surcharger les radars du navire
- contrôler les moteurs et la vitesse du navire
- déstabiliser les navires par le transfert ou l'inondation des eaux de ballast
- endommager gravement l'équipement en mettant, par exemple, hors service un système de refroidissement vital
- arrêter les systèmes vitaux de la cargaison tels que l'alimentation électrique des réfrigérateurs
- arrêter les systèmes de détection et d'extinction des incendies
- prendre le contrôle du gouvernail suffisamment longtemps pour diriger le navire à pleine vitesse vers un quai

Les navires doivent donc avoir recours à des solutions technologiques et des principes opérationnels pour éviter ce type de situations. Les solutions sont décrites dans cette étude aux chapitres 5 et 6.

Il en va de même pour les ports, où les systèmes TI et TO sont également utilisés en permanence. Dans le domaine de la sécurité des ports et des terminaux conformes à l'ISPS, il est important de prendre en compte les éléments suivants :

- le système de gestion de la sécurité (SeMS) n'est efficace que s'il est numérisé.

- le système de badges d'identification est efficace lorsqu'il s'agit d'un système numérique qui s'appuie sur une base de données commune à laquelle les forces de l'ordre et les douanes ont également accès.
- le système de barrière automatique ne doit admettre que les personnes autorisées à entrer dans la zone.
- un système de surveillance du périmètre doté d'un système de télévision en circuit fermé (CCTV) ou d'un autre système de caméras très performant doit pouvoir prendre des mesures intelligentes et suivre les séquences vidéo pendant de longues périodes.

Vous trouverez plus de détails à ce sujet ci-dessous.

4.4.2.4 L'utilisation d'ordinateurs pour communiquer entre les parties prenantes permet d'agir efficacement et en temps réel lorsque cela est nécessaire. Chaîne d'approvisionnement et menaces hybrides

Les chaînes d'approvisionnement maritimes sont les veines du commerce et de l'économie mondiale. Elles s'appuient sur une collaboration transfrontalière pour offrir des services complexes et essentiels (par ex., la gestion des conteneurs, le transport de véhicules, le stockage et le transport de GNL, les croisières). La plupart des processus physiques au sein d'un service maritime (les véhicules, le chargement/déchargement des marchandises, la distribution et le stockage du GNL) sont exécutés par des systèmes mécaniques et des machines autonomes ou semi-autonomes (comme les navires, les camions, les grues, les barrières/clôtures électroniques) sous le contrôle de logiciels sophistiqués chargés de traiter la chaîne logistique (à savoir, des systèmes industriels physiques et informatiques, des SCADA, des systèmes de surveillance). En outre, les navires cargo sont reliés aux ports et aux autres opérateurs par une multitude de liaisons de communication et de données (communications par satellite ou communications radio conventionnelles). Par ailleurs, leur navigation est aujourd'hui largement tributaire de solutions électroniques (navigation par satellite avec GPS, Galileo ou systèmes électroniques de visualisation des cartes marines (ECDIS)). Ainsi, les chaînes d'approvisionnement maritimes peuvent être considérées comme des systèmes complexes composés d'installations hétérogènes et interconnectés appartenant à différentes infrastructures critiques nationales, européennes et internationales. Ces dernières garantissent un échange rapide et sans heurts de produits et de données entre le producteur et le consommateur final pendant la prestation de ces services.

L'interconnexion des installations physiques et informatiques expose l'écosystème maritime à des **menaces hybrides** où les attaques sur les installations physiques se propagent aux installations informatiques, et inversement**.**

Les attaques contre les services de la chaîne d'approvisionnement maritime engendrent non seulement une perturbation des services, mais affectent aussi de manière considérable les opérations maritimes, la sécurité internationale, les économies, les sociétés et l'environnement. Ainsi, les attaques contre les systèmes contrôle-commande industriels (ICS) (outils de supervision, SCADA, systèmes de contrôle distribués et contrôleurs logiques programmables) hébergés dans les ports ou les entreprises de transport maritime peuvent perturber ou endommager des dispositifs mécaniques critiques (grues à conteneurs,

systèmes de sécurité et systèmes mécaniques qui font fonctionner les écluses et les barrages). Pire encore, ces attaques peuvent entraîner des pertes de vies humaines, des vols de cargaisons ou la destruction d'un navire. En cas de piratage d'un système SCADA, les effets (en termes de rayonnement thermique, d'onde de choc de surpression et d'éclats d'obus) de l'explosion d'un navire-citerne de GNL, d'installations de stockage de GNL ou de terminaux portuaires sont assez dévastateurs pour conduire à une perte de réserve d'énergie, ce qui pourrait être critique pendant la période hivernale. L'explosion pourrait également avoir un impact négatif sur l'environnement (dégradation, fragmentation ou perte d'écosystèmes), sur l'économie et, plus important encore, sur le bien-être et la santé des citoyens. Une attaque contre le système de gestion d'un terminal à conteneurs a le potentiel de perturber les services intermodaux de transport de conteneurs, qui s'appuient sur le transport maritime, ferroviaire et routier.

Les cyberattaques (comme l'insertion d'un logiciel malveillant) dans les systèmes SCADA des ports peuvent provoquer des déversements de carburant pouvant affecter la qualité de l'eau ; les attaques sur le PCS peuvent transformer les méthaniers en bombes flottantes ; les attaques physiques (comme les bombardements) dans une zone de stockage en vrac de produits houillers peuvent générer des vents de poussière pouvant atteindre des zones touristiques ou des habitations voisines. Les systèmes de surveillance modernes, les unités de contrôle, les capteurs, les RFID, les systèmes de trafic maritime, les PCS et les procédures automatisées de contrôle aux frontières sont sensibles aux menaces actuelles. Ils peuvent être victimes d'espionnage, d'interruption, de vandalisme et d'interception, ce qui peut entraîner la perturbation de divers services et opérations maritimes essentiels. Leur détournement peut être utilisé pour le trafic d'êtres humains et de stupéfiants, mais aussi pour commettre des actes terroristes. Il convient de noter que selon les estimations de 2016 de la RAND Corporation et du Congressional Research Service des États-Unis, toute attaque contre une infrastructure critique portuaire pourrait causer des dizaines de milliers de morts et paralyser le commerce mondial. Les pertes économiques subies pourraient aller de 45 milliards de dollars à plus de 1 000 milliards de dollars.

En 2015, l'International Port Community Systems Association (IPCSA) a recommandé que tous les acteurs du secteur maritime, de la logistique et de la chaîne d'approvisionnement, ainsi que les opérateurs de PCS (avec le soutien de leurs associations professionnelles et des organismes internationaux et régionaux), s'attaquent aux menaces qui pèsent actuellement sur la chaîne d'approvisionnement. En outre, l'association a recommandé de réunir les principaux acteurs de la chaîne d'approvisionnement pour créer un centre de partage et d'analyse de l'information (ISAC), afin de discuter des menaces, des risques et des expériences en matière de cybersécurité.

L'ENISA a publié les principales menaces pesant sur la chaîne d'approvisionnement. Elles sont présentées ci-dessous.[29]

[29] (Threat Landscape for Supply Chain Attacks, 2021)

FOURNISSEUR		CLIENT	
Techniques d'attaque utilisées pour compromettre la chaîne d'approvisionnement	Actifs des fournisseurs ciblés par l'attaque de la chaine d'approvisionnement	Techniques d'attaque utilisées pour compromettre le client	Activos del cliente objeto del ataque a la cadena de suministro
Infection par un logiciel malveillant Ingénierie sociale Attaque de force brute Exploiter d'une vulnérabilité logicielle Exploiter d'une vulnérabilité de configuration Renseignement de sources ouvertes (OSINT)	Logiciel préexistant Bibliothèques de logiciels Code Configuration Donnés Processus Matériel informatique Personnes Fournisseur	Relation de confiance [T1199] Compromis « Drive-by » [T1189] Hameçonnage [T1566] Infection par un logiciel malveillant Attaque ou modification physique Contrefaçon	Donnés Données personnelles Propriété intellectuelle Logiciel Processus Bande passante Financier Personnes

Image 7: Taxonomie des attaques contre les chaînes d'approvisionnement proposée par l'ENISA.

On retrouve quatre parties : (i) les techniques d'attaque utilisées contre le fournisseur, (ii) les installations du fournisseur qui sont attaquées, (iii) les techniques d'attaque utilisées contre le client, (iv) les installations du client qui sont attaquées.

4.4.2.5 Vecteurs de menace

Sur la base de nombreuses ressources [30, 31, 32, 33, 34 et 35], les menaces courantes en matière de cybersécurité maritime et les installations maritimes visées par des techniques spécifiques sont énumérées ci-dessous :

Menaces :	Techniques :	Les installations et services maritimes pris pour cible :
Ransomware	Accès initial	Personnes, systèmes informatiques, appareils informatiques, composants de réseau et de communication, informations et données, etc.
	Exécution	Systèmes informatiques, appareils informatiques, composants de réseau et de communication, etc.
	Persistance	Personnes, services administratifs, services d'appui, etc.

[30] (Ashraf, et al., 2022)
[31] (ENISA Threat Landscape 2022, 2022)
[32] (Guidelines - Cyber Risk Management for Ports, 2020)
[33] (Alcaide & Garcia-Llave, 2020)
[34] (Meland, Bernsmed, Wille, Rødseth, & Nesheim, 2021)

	Escalade des privilèges	Personnes, systèmes informatiques, appareils informatiques, etc.
	Évasion (détournement des équipements de détection d'intrusion)	Systèmes informatiques, appareils informatiques, composants de réseau et de communication, infrastructure mobile, infrastructure fixe, etc.
	Accès aux identifiants	Personnes, systèmes informatiques, appareils informatiques, etc.
	Discovery	Personnes, systèmes informatiques, appareils informatiques, composants de réseau et de communication, etc.
	Mouvement latéral	Personnes, systèmes informatiques, appareils informatiques, composants de réseau et de communication, informations et données, etc.
	Collecte	Informations et données, services d'accostage des navires, services de sécurité et de sûreté, personnel, services d'appui, services de stockage temporaire et de séjour, services de distribution et de transfert, etc.
	Commande et contrôle	Systèmes informatiques, appareils informatiques, composants de réseau et de communication, informations et données, services d'accostage des navires, services de chargement et de déchargement des navires, services de distribution et de transfert, infrastructure mobile, infrastructure fixe, systèmes et réseaux TO, etc.
	Exfiltration	Appareils informatiques, systèmes informatiques, composants de réseau et de communication, systèmes et réseaux TO, etc.
	Impact	Systèmes informatiques, appareils informatiques, composants de réseau et de communication, informations et données, etc.
Logiciels malveillants	Brèche de sécurité	Appareils informatiques, systèmes informatiques, informations et données, etc.
Ingénierie sociale	Reconnaissance	Personnes, systèmes informatiques, services administratifs, services de sécurité, systèmes de sécurité, etc.
	Développement des ressources	Personnes, systèmes informatiques, services administratifs, systèmes de sécurité, informations et données, etc.
	Accès initial	Personnes, systèmes informatiques, systèmes et réseaux TO, appareils TO, appareils TO, etc.
	Exécution	Personnes, systèmes informatiques, etc.
Menaces contre la disponibilité (DDoS)	Développement des ressources	Systèmes informatiques, appareils informatiques, composants de réseau et de communication, informations et données, infrastructure mobile, infrastructure fixe, etc.
	Évasion (détournement des équipements de détection d'intrusion)	Systèmes informatiques, appareils informatiques, composants de réseau et de communication, etc.
	Impact	Systèmes informatiques, appareils informatiques, composants de réseau et de communication, informations et données, infrastructure mobile, infrastructure fixe, services d'accostage des navires, services de chargement et de

		déchargement des navires, services de distribution et de transfert, services d'assistance, services administratifs, services de sécurité, etc.
Menaces contre la disponibilité (menaces Internet)	Accès initial	Appareils informatiques, systèmes informatiques, composants de réseau et de communication, etc.
	Discovery	Appareils informatiques, systèmes informatiques, composants de réseau et de communication, etc.
	Collecte	Appareils informatiques, systèmes informatiques, composants de réseau et de communication, etc.
	Impact	Appareils informatiques, systèmes informatiques, composants de réseau et de communication, etc.
Désinformation - Information erronée	Reconnaissance	Personnes, appareils informatiques, systèmes informatiques, informations et données, etc.
	Développement des ressources	Personnes, appareils informatiques, systèmes informatiques, informations et données, etc.
	Accès initial	Personnes, appareils informatiques, systèmes informatiques, etc.
	Exécution	Personnes, appareils informatiques, systèmes informatiques, etc.
	Impact	Personnes, appareils informatiques, systèmes informatiques, etc.
Attaques contre les chaînes d'approvisionnement	Reconnaissance	Fournisseurs et clients (tableau de l'ensemble des menaces pour les attaques sur les chaînes d'approvisionnement)
	Développement des ressources	Fournisseurs et clients (tableau de l'ensemble des menaces pour les attaques sur les chaînes d'approvisionnement)
	Accès initial	Fournisseurs et clients (tableau de l'ensemble des menaces pour les attaques sur les chaînes d'approvisionnement)

5 Normes et stratégies en matière de sécurité maritime

Ce chapitre présente les organisations de normalisation et les organes politiques, ainsi que les normes de sécurité maritime (sûreté et cybersécurité) et leurs objectifs.

5.1 Introduction

Depuis plus d'une décennie, des efforts considérables ont été déployés pour introduire des méthodes de gestion des risques et d'assurance pour les IIC. Ces dernières se concentrent soit sur les cybermenaces soit sur les menaces physiques, sans tenir compte de la double nature complexe (physique et informatique) des IIC maritimes. Ce chapitre résume les normes de sécurité maritime pertinentes. La dernière section présente des conseils sur ce qu'il convient d'utiliser en fonction de la menace rencontrée.

5.1.1 Stratégie de sûreté maritime de l'Union européenne (SSMUE)

La première stratégie de sûreté maritime a été adoptée le 24 juin et le 16 décembre 2014 en réponse aux risques et menaces modernes pesant sur la sûreté maritime mondiale. La stratégie promeut une meilleure coopération civile et militaire ainsi qu'une meilleure coordination entre les acteurs de la sécurité intérieure et extérieure, tels que la police et la défense. L'objectif est que cette approche commune de la sûreté maritime favorise une coopération plus étroite entre les différents secteurs maritimes, et rende la politique de sûreté maritime de l'UE plus cohérente, plus efficace et moins coûteuse. Cette boîte à outils explique comment le plan d'action doit être mis en œuvre. En outre, il met en évidence les activités du Service européen pour l'action extérieure (SEAE), le rôle des délégations de l'UE et des services du siège du SEAE.

La stratégie révisée de l'UE en matière de sûreté maritime, adoptée en juin 2018, prévoit un processus d'établissement de rapports plus ciblé afin de renforcer la sensibilisation et d'assurer un meilleur suivi de la stratégie initiale. Le plan d'action regroupe les aspects internes et externes de la sûreté maritime communautaire, facilite une approche stratégique et intersectorielle, et établit un programme civil et militaire commun pour la recherche sur la sûreté maritime (dont le double usage).

La stratégie révisée souligne qu'une meilleure coordination devrait être assurée dans le cadre de la mise en œuvre des stratégies et politiques de l'UE ayant des objectifs transversaux, tels que ceux figurant dans les domaines de l'énergie, de l'environnement et de la sécurité. Dans ce dernier domaine, l'accent est mis sur les menaces et les défis, dont les menaces informatiques et hybrides, le terrorisme et la criminalité organisée. Cette stratégie met en avant la nature changeante des menaces dans le domaine maritime et appelle à un engagement renouvelé en faveur de la protection des infrastructures maritimes critiques, y compris sous-marines, et des infrastructures de transport maritime, d'énergie et de communication. Pour ce faire, cette stratégie propose notamment de renforcer la conscience maritime grâce à une meilleure interopérabilité et à un échange d'informations rationalisé (obligatoire et volontaire). Elle appelle à améliorer la protection et la résilience des systèmes et infrastructures maritimes. À cet égard, les politiques et initiatives pertinentes de l'UE sont prises en compte.

L'une des principales actions mentionnées est la révision du point A.3.8 : « Garantir une meilleure intégration de la cybersécurité dans le domaine maritime en termes de capacités, de recherche, de technologie et d'industrie, en s'appuyant sur la coordination civilo-militaire et les synergies avec les politiques de l'UE liées à la cybersécurité et à la cyberdéfense, conformément à la directive NIS et aux recommandations et réglementations internationales telles que SOLAS XI-2 et le code ISPS, ainsi qu'à leurs futures mises à jour. Il s'agira notamment d'échanger les meilleures pratiques et de développer des projets communs entre les États membres de l'UE sur la prévention des cyberattaques maritimes ».

L'action A.4.3 prévoit de « poursuivre une approche globale de la gestion des risques en matière de sécurité maritime, en procédant notamment à une analyse commune des risques et en identifiant les lacunes et les chevauchements éventuels dans ce domaine, tout en tenant compte des cybermenaces et des menaces hybrides, des défis climatiques, et des catastrophes maritimes et environnementales. »

L'action A.4.8 stipule : « Mettre en place un réseau d'experts en matière de cybersécurité et de cyberdéfense dans le domaine maritime afin d'élaborer des lignes directrices sur les procédures à suivre en réponse aux nouvelles menaces dans le domaine maritime, y compris les éventuels actes de terrorisme et autres actes illicites intentionnels en mer. Il est question notamment de la protection des navires, de la cargaison, de l'équipage et des passagers, des ports et des installations portuaires, des installations énergétiques marines et d'autres infrastructures maritimes et énergétiques essentielles, conformément à la directive NIS et au code ISPS. » Le renforcement des capacités et l'amélioration de l'enseignement et de la formation à la cybersécurité dans le domaine maritime, en collaboration avec toutes les parties prenantes (les Nations unies, l'Organisation internationale du travail (OIT), l'OMI et l'OTAN) figurent également parmi les actions de la stratégie révisée (actions A.5.1, A.5.6).

La SSMUE couvre les aspects internes et externes de la sûreté maritime de l'Union et contribue à la stabilité et à la sécurité du domaine maritime mondial, conformément à la stratégie européenne de sécurité. La Direction générale (DG) MARE est l'organe de la Commission européenne responsable du développement de la stratégie. Elle collabore avec diverses DG (la DG CNECT, la DG MOVE, la DG ECHO, la DG RTD) et agences (l'Agence européenne pour la sécurité maritime (AESM), l'ENISA). La stratégie 2020 de l'Union européenne pour la sécurité promeut l'autonomie stratégique et la résilience des chaînes d'approvisionnement de l'UE en termes de produits, de services, d'infrastructures et de technologies critiques.

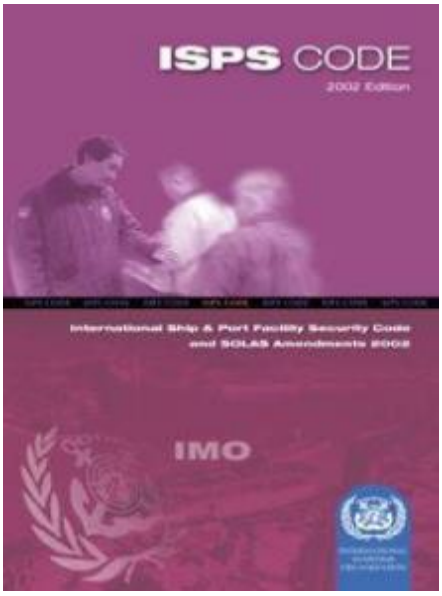
5.1.2 Normes en matière de sûreté maritime

Les organisations maritimes (OMI, BIMCO, AESM, entre autres) ont publié diverses normes et lignes directrices relatives à la sûreté, dont plusieurs sont détaillées ci-dessous.

5.1.2.1 Le code ISPS

La plus importante de ces normes est le Code international pour la sûreté des navires et des installations portuaires (ISPS), qui a été établi par l'OMI dans le cadre de la convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS) de 1974 (chapitre XI-2).[35]

[35] (SOLAS XI-2 and the ISPS Code, n.d.)



Le code ISPS fournit un cadre dans lequel les navires et les installations portuaires peuvent coopérer pour détecter et décourager les actes qui constituent une menace pour la sûreté maritime. Le code propose une approche pour établir une gouvernance de la sûreté dans les infrastructures maritimes critiques. Le code ISPS :

- permet de détecter et de dissuader les menaces pour la sûreté dans un cadre international ;
- définit les rôles et les responsabilités ;
- permet la collecte et l'échange d'informations sur la sûreté;
- fournit une méthode d'évaluation de la sûreté;
- veille à ce que des mesures de sûreté adéquates soient mises en place.

Le code est composé de deux parties dans lesquelles figurent des exigences obligatoires et des lignes directrices pour la sûreté des navires et des installations portuaires. La partie A traite des exigences obligatoires et la partie B des recommandations de mise en œuvre pour renforcer la sûreté. À cet égard, les principes qui sous-tendent le code ISPS sont comparables au code ISM à bord d'un navire. Avant que le code ISPS ne soit légalement applicable dans un pays, il doit être transposé dans la législation nationale. Certains pays ont adopté le code ISPS peu après juillet 2004, mais d'autres ne l'ont fait que des années plus tard. Certains pays ont adopté le code dans son intégralité, tandis que d'autres ont apporté des modifications au code ISPS dans sa version nationale concernant certains aspects de la sûreté portuaire.

L'Union européenne[36] a immédiatement mis en œuvre la partie A du code dans ses ports et a décidé de considérer la partie B comme obligatoire plutôt que comme une simple recommandation. Les pays africains ont mis en œuvre le code de manière indépendante par le biais de leur législation nationale.

[36] Directive 2005/65/CE relative à l'amélioration de la sûreté des ports et des zones adjacentes

Il est important de souligner que le code ISPS utilise le terme « installation portuaire », ce qui signifie que le port n'est pas couvert par le code. Les aspects de la sûreté « portuaire » sont abordés dans le code de bonne pratique (COP) sur la sûreté dans les ports.

La convention de Genève de 2003 sur la sûreté portuaire complète les dispositions du code ISPS en ce qui concerne la sûreté de la zone portuaire au sens large. Le code définit les fonctions, les tâches et les mesures de sécurité visant à dissuader les actes criminels contre les ports et à y répondre. Il utilise les mêmes pratiques et principes que le code ISPS et constitue un guide pour la sûreté portuaire au-delà de la zone des installations portuaires. L'Union européenne a introduit le code en tant que ligne directrice obligatoire[37] pour améliorer la sûreté de ses ports.

5.1.2.1.1 Sûreté en matière de construction

Dès la construction d'un navire, la sûreté commence par une première exigence : un navire doit être en état de naviguer avant de quitter le rivage, comme l'exige le Lloyds of London (P&I Club).[38] Chaque navire marchand est enregistré par l'État du pavillon, qu'il s'agisse du pays de résidence de l'armateur ou du pays battant pavillon de complaisance. Ils doivent être conformes aux règles, réglementations et dispositions maritimes de l'État du pavillon concerné, ainsi qu'aux règles et dispositions maritimes internationales de l'OMI. Ils doivent également être certifiés par une société de classification.

Toutefois, certains pavillons de complaisance ont réduit les critères de sûreté, ne disposent pas de ressources suffisantes pour effectuer des inspections adéquates et n'imposent pas de sanctions aux navires en infraction. Résultat : des navires qui ne satisfont pas à plusieurs exigences critiques en matière de sûreté sont parfois autorisés à accoster dans certains ports. Étant donné que les propriétaires de ces navires peu sûrs se concentrent uniquement sur la réparation des parties défectueuses lorsque des défauts apparaissent plutôt que sur l'entretien préventif, le risque d'accident est élevé.

5.1.2.1.2 Contrôle des navires par l'État du port (PSC)

Il incombe à l'État du pavillon (le pays où le navire est enregistré) de veiller à ce que ce dernier réponde à toutes les normes de sûreté requises. Le PSC constitue un soutien efficace aux inspections effectuées régulièrement par les États du pavillon pour détecter les navires qui ne répondent pas aux normes.

Le PSC est l'initiative de l'OMI en matière de sûreté maritime (sécurité physique) qui a pour objectif de vérifier la conformité d'un navire avec les conventions et les normes internationales. Elles contribuent à réduire les risques liés aux navires. Le rôle du PSC est de mettre en évidence les risques potentiels en matière de sécurité (sûreté et cybersécurité) et d'en informer l'État du pavillon du navire. Lors des inspections de navires, le PSC permet de vérifier que l'état du navire et de son équipement de manutention est conforme aux exigences des règlements internationaux de l'OMI. Ces inspections permettent également de s'assurer que le navire dispose d'un équipage et qu'il est exploité conformément à ces règles.

[37] Directive 2005/65/CE relative à l'amélioration de la sûreté des ports et des zones adjacentes
[38] (Rulebook 2021)

Elles obéissent à une résolution de coopération pour les contrôles des navires et des déchargements (Résolution 682 17 de l'OMI).[39]

5.1.2.1.3 Normes d'exploitation pour garantir la sûreté des navires

Les marins représentent le facteur humain qui permet de limiter les risques à bord. Ce rôle incombe au responsable de la sûreté à bord, qui est chargé de tenir à jour le plan de gestion de la sûreté, d'avoir recours à un système de gestion de la sûreté (SMS) et de maintenir l'équipage en alerte au moyen de formations. L'épine dorsale de cette gouvernance est le système de gestion de la sûreté, dont l'objectif principal est de fournir une approche systématique de la gestion des risques de sûreté dans l'exploitation des navires. Le SMS fait partie du code international de gestion de la sécurité (ISM)[40] et les navires commerciaux sont tenus par l'OMI de mettre en place des procédures de gestion sûre des navires.

L'un des aspects les plus importants du maintien de l'intégrité du navire au cours d'un voyage en mer est le bon arrimage de la cargaison. Les forces latérales et longitudinales exercées sur le navire par la houle pendant les tempêtes représentent un risque énorme pour la stabilité du navire en raison des risques de déplacement de la cargaison. Toutes les cargaisons doivent être arrimées et sécurisées de manière à ne pas mettre en danger le navire et son équipage. Des procédures d'arrimage et de fixation appropriées doivent être suivies, conformément au code CSS de l'OMI.[41] Si, à la suite d'une attaque malveillante, la cargaison n'est plus sécurisée et peut bouger librement dans la cale, il existe un risque réel de perte du navire et de l'équipage.

5.1.2.1.4 Prévention et réaction en matière de sûreté à bord des navires

En cas d'accident à bord, il est essentiel que l'équipage soit formé pour minimiser immédiatement l'impact des dommages subis. C'est pourquoi les membres de l'équipage sont formés aux principes de gestion de crise et aux procédures d'intervention d'urgence pour tous les types d'accidents, ainsi qu'à la lutte contre les incendies. Le code de formation des gens de mer, de délivrance des brevets et de veille (STCW)[42] et la convention SOLAS traitent de ces aspects en détail, mais ce domaine d'expertise n'entre pas dans le cadre de la présente étude.

5.1.2.2 Autres codes importants

- Code maritime international des cargaisons solides en vrac (code IMSBC) de l'OMI ;
- Recueil international de règles relatives à la construction et à l'équipement des navires transportant des produits chimiques dangereux en vrac (Recueil IBC) ;
- Recueil international de règles de sécurité pour le transport de grains en vrac (International Grain Code) ;
- Recueil de règles pratiques pour la sécurité du chargement et du déchargement des vraquiers (Recueil BLU) ;
- Code maritime international des marchandises dangereuses (Code IMDG) ;

[39] (Resolution A.682 (17), 1991)
[40] (The International Safety Management (ISM) Code)
[41] (Code of Safe Practice for Cargo Stowage and Securing (CSS Code), n.d.)
[42] (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 197, n.d.)

- L'AESM[43] fournit des outils aux acteurs maritimes de l'UE, tels que l'AIS et SafeSeaNet pour le suivi du trafic maritime ; CleanSeaNet pour les images satellite à des fins d'identification de la pollution en mer ; l'EMCIP pour la centralisation des données sur les accidents maritimes, les outils de formation, etc.
- L'Organisation européenne des ports maritimes[44] fait la promotion des ports verts et des efforts en matière d'efficacité énergétique. Elle est spécialisée dans les lignes directrices concernant la sécurité et la formation relative aux opérations des navires dans les ports, à savoir : le ravitaillement en GNL, la réception des déchets, le chargement et déchargement de marchandises générales, de conteneurs et de vrac, et les mouvements de conteneurs.
- L'OIT[45] a publié le Recueil de directives pratiques sur la sécurité et la santé dans les ports. Ce recueil fournit des orientations pertinentes pour la gestion, l'exploitation, l'entretien et le développement des ports.
- L'initiative des douanes américaines sur la sécurité des conteneurs (ISC)
- Partenariat Douanes-Commerce contre le terrorisme (C-TPAT)
- Plan de sécurité de l'équipage
- Système de manifeste automatisé (AMS)
- SafeSeaNet
- AIS

5.1.3 Normes en matière de cybersécurité

5.1.3.1 Normes[46] ISO pour la sécurité des IIC maritimes

La norme ISO27000 définit les concepts de sécurité. La norme ISO/IEC 27001 traite des exigences de sécurité physique en termes de prévention contre les accès non autorisés aux informations d'une organisation et de ses installations pertinentes. Elles sont divisées en deux grandes catégories : les zones sécurisées et la sécurité des équipements.

La norme ISO/IEC 27001 traite également du système de gestion de la sécurité de l'information (SGSI) d'une organisation, qui, dans le cas du présent rapport, est l'IIC du port. En pratique, la conformité à la norme ISO 27001 signifie que l'organisation, dans notre cas le port, répond aux exigences de la norme dans le domaine de la sécurité. Cet aspect est primordial pour le bon fonctionnement du port afin que ce dernier puisse se prémunir contre les cybermenaces. Les IIC sont bien protégées. En outre, elle clarifie les termes de la sécurité physique, tels que le périmètre de sécurité physique, les contrôles d'entrée physique et les infrastructures. Les exigences en matière de sécurité physique sont également définies dans la publication spéciale 800-171 du NIST. Les normes de la famille ISO2800x fournissent des lignes directrices pour la sécurité de la chaîne d'approvisionnement, en particulier pour les

[43] (European Maritime Safety Agency , n.d.)
[44] (ESPO: The First Port of Call for European Transport Policy Makers in Brussels, n.d.)
[45] (ILO: International Labour Oeganization, n.d.)
[46] (Standards, n.d.)

chaînes d'approvisionnement maritimes. Le tableau suivant[47] résume les différentes normes ISO relatives à la sécurité maritime.

Numéro	ISO	COMMENTAIRES
1.	ISO 18788:2015	Système de gestion des opérations de sécurité privée
2.	ISO 9001 / BS 10800	Code de bonne pratique pour la fourniture de services de sécurité
3.	ISO/IEC 27001	Norme internationale de gestion de la sécurité de l'information
4.	ISO 27002:2013 (anciennement ISO 17799:2000)	Norme globale de sécurité de l'information. Elle est composée de quatorze sections (5 à 18), chacune étant structurée de la même manière
5.	ISO/IEC TS 30104:2015	Technologies de l'information - Techniques de sécurité - Attaques de sécurité physique, techniques d'atténuation et exigences de sécurité
6.	ISO 28000:2007	Spécifie les exigences relatives à un système de gestion de la sûreté, y compris les aspects essentiels à la garantie de la sûreté de la chaîne d'approvisionnement.
7.	ISO 28000:2022	Sécurité et résilience - Systèmes de gestion de la sécurité - Exigences

Étant donné que les navires autonomes et les applications maritimes innovantes font appel à l'IA, il convient de prendre en compte plusieurs normes supplémentaires pour développer un écosystème maritime basé sur l'IA et fiable.

Les principales normes relatives à l'IA sont mentionnées ci-dessous :

5.1.3.2 Normes ISA, ANSI pour les ACS

Les normes ISA et ANSI visent la sécurité des systèmes de contrôle-commande industriels (ACS, par ex., SCADA). Voici quelques exemples de ces normes :

- ISA-TR62443-2-3-2015 Sécurité des systèmes de contrôle-commande industriels, Partie 2-3 : Gestion des correctifs dans l'environnement IACS
- ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 Sécurité des systèmes de contrôle-commande industriels, Partie 2-4 : Exigences du programme de sécurité pour les fournisseurs de services IACS (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT)
- ANSI/ISA-62443-3-2-2020 Sécurité des systèmes de contrôle-commande industriels, Partie 3-2 : Évaluation des risques de sécurité pour la conception des systèmes
- ANSI/ISA-62443-4-1-2018 Sécurité des systèmes de contrôle-commande industriels, Partie 4-1 : Exigences relatives au cycle de développement de produit sécurisé

5.1.3.3 Catégorisation des normes

Il existe de nombreuses normes de sécurité émanant de divers organismes de normalisation (ISO, OMI, ETSI, NIST, BIMCO, IEEE) qui traitent de différents sujets. Ces efforts fragmentés créent une certaine confusion concernant la ou les normes à adopter. Les complémentarités

[47] (Y. Papagiannopoulos, "Standards in Practice", IEEE Conference on Standards for Communications and Networking, novembre 2022.)

et les chevauchements doivent être clarifiés. Pour contribuer à cette clarification, une classification des normes[48] a été établie. Ces dix catégories de normes y ont été identifiées :

1. Vocabulaire et conceptualisation : normes pouvant être utilisées pour définir des terminologies et décrire des concepts.
2. Exigences en matière de sécurité : normes fixant des exigences en matière de sécurité.
3. Lignes directrices en matière de sécurité : normes qui fournissent des bonnes pratiques.
4. Évaluation de la sécurité : normes et bonnes pratiques relatives à l'évaluation ou aux méthodes d'évaluation de la sécurité.
5. Confidentialité et protection des données : normes relatives au maintien de la confidentialité et de la protection des données.
6. Normes de gestion des risques : normes et bonnes pratiques qui fournissent des principes, des cadres ou des processus liés à la gestion des risques de sécurité.
7. Normes techniques : normes portant sur les aspects techniques de la sécurité.
8. L'IA et la sécurité : On y retrouve des normes, des cadres et des bonnes pratiques liés à la sécurité en matière d'IA (important pour les navires autonomes, les noyades en mer).
9. Normes sectorielles (le transport maritime, entre autres) : normes de gestion de la sûreté qui répondent aux exigences et aux spécificités d'un secteur particulier (par ex., les systèmes communautaires portuaires).
10. Protection des infrastructures critiques : normes relatives à la protection des infrastructures essentielles à la durabilité de l'économie et au bien-être social (par ex., les infrastructures maritimes critiques).

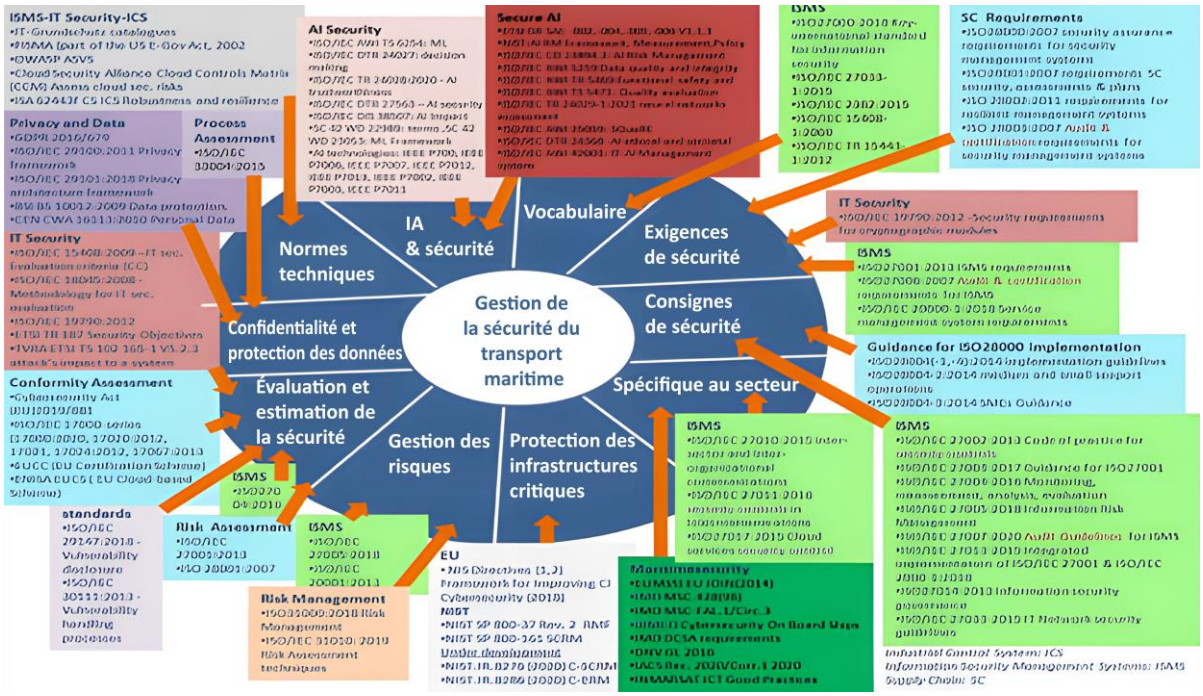


Image 8: Taxonomie des normes de sécurité maritime[49]

[48] (Kalogeri & Polemi, 2022)
[49] *Ibid.*

5.2 Législation en matière de sûreté

Les règles de sûreté dans les ports du monde entier (y compris en Afrique) ne sont en principe pas entièrement régies par les normes internationales et restent du ressort de l'État souverain. Chaque pays a établi ses propres règles de sûreté, ce qui a donné lieu à un éventail de lois parfois différentes et obsolètes.

Les principes de sécurité de la gouvernance portuaire sont essentiels, car ils impliquent de nombreux décideurs et parties prenantes tels que l'autorité portuaire, les opérateurs de terminaux, les opérateurs ferroviaires, les entreprises de camionnage, les fournisseurs de services logistiques et les services d'urgence. Les aspects généraux de la sûreté liés à la zone portuaire et à la manutention des marchandises doivent être pris en compte lors de l'élaboration d'un système de gestion de la sûreté portuaire. Il ne serait pas possible de rendre justice au sujet ici, mais il existe un facteur commun : sûreté rime avec infrastructures et équipements de manutention de qualité, personnel bien formé, ensemble de procédures bien pensées et SMS capable de contrôler et suivre la situation réelle en matière de sûreté. Il incombe aux responsables du port et des installations de gérer leur SMS de manière professionnelle afin d'éviter tout dommage ou toute atteinte aux personnes. Le bouclier de sécurité ne doit pas être fragilisé, car cela pourrait engendrer des dégâts suite à des cyberattaques ou à des attaques sur les infrastructures de sécurité.

La plupart des législations dans le domaine maritime ont été établies suite à une catastrophe maritime. Le cas échéant, la catastrophe du Titanic a conduit à la création de la réglementation internationale de sécurité SOLAS de 1974. Elle avait pour objectif d'agir comme un « bouclier de sécurité », afin de protéger les marins et les navires. L'importante couverture médiatique, le choc mondial provoqué par le bilan humain élevé et le procès intenté par les survivants à la « White Star Line » ont conduit à des améliorations significatives de la sûreté en mer.

En plus de cette pression sociale, les compagnies d'assurance maritime ont forcé les compagnies maritimes à faire preuve de plus d'initiative dans la prévention des accidents et ont convaincu les gouvernements de mettre en place des lois plus efficaces en matière de sûreté. Nous sommes passés d'une logique de fuite en avant et de paiement de dommages-intérêts à une mentalité de sensibilisation à la sûreté et de prévention. Cette nouvelle mentalité est primordiale pour la sauvegarde de vies humaines, moins coûteuse pour les compagnies d'assurance et plus efficace pour les armateurs. Le monde maritime reste un secteur à haut risque, dont les conséquences sont considérables en cas d'incident.

L'amélioration la plus importante a été la création de la convention SOLAS, qui a établi des principes et des règles uniformes pour la construction, l'installation et l'exploitation des navires marchands. La version actuelle de la convention SOLAS de 1974[50] est encore aujourd'hui la norme mondiale pour les navires et les marins. Chaque pays, chaque port et chaque situation locale sont différents et exigent une approche complexe et personnalisée

[50] (International Convention for the Safety of Life at Sea (SOLAS), 1974, n.d.)

des risques pour toutes les opérations, afin d'atténuer et de minimiser les risques en matière de sûreté. Certains pays, comme l'Australie, encouragent une approche personnalisée de la gestion de la sûreté dans les ports. Ils se contentent de fournir des conseils sur les bonnes pratiques et d'esquisser un modèle permettant de mesurer les politiques, les procédures et les performances des opérations portuaires.

Étant donné que chaque port présente des risques de sûreté qui lui sont propres, les règles de gestion ne peuvent être abordées qu'à l'intérieur du port en question et en utilisant les réglementations, les lignes directrices et les meilleures pratiques internationales comme outil d'amélioration de la sûreté. Une réglementation internationale unique et uniforme en matière de sécurité n'est pas possible dans le monde d'aujourd'hui, notamment parce que certains pays ne disposent pas des connaissances de base en matière de sûreté.
Contrairement à ce règlement sur la sûreté, la création d'une « législation sur la sécurité » a été entreprise suite à une catastrophe terrestre, lorsque des avions détournés ont percuté les tours jumelles du World Trade Center le 11 septembre 2001.

Le secteur maritime est aujourd'hui régi par plusieurs réglementations qui obligent les opérateurs maritimes à assurer la sécurité et la sûreté des navires. Ces règles s'appliquent également à la cybersécurité. D'ailleurs, avec la résolution MSC.428(98) de l'OMI, les risques liés à la cybersécurité doivent désormais être pris en compte dans le système de gestion de la sûreté (SMS). Selon les Directives de l'OMI sur la gestion des cyber-risques maritimes (MSC-FAL.1 Circ.3), [51] « ...le cyber-risque maritime se réfère à une situation dans laquelle une infrastructure technologique est menacée par une circonstance ou un événement potentiel qui pourrait entraîner des défaillances opérationnelles, de sécurité ou de sûreté liées à la navigation en raison d'endommagement, de pertes ou de compromissions des systèmes informatiques. »

Outre les directives de l'OMI, l'Association internationale des ports (IAPH) a également élaboré un ensemble de lignes directrices sur la cybersécurité à l'intention des ports et des installations portuaires.[52]

Voici quelques-unes des réglementations européennes spécifiques en matière de sûreté portuaire :

- Directive 2000/59/CE du Parlement européen et du Conseil du 27 novembre 2000 sur les installations de réception portuaires pour les déchets d'exploitation des navires et les résidus de cargaison.
- Directive 2001/96/CE du Parlement européen et du Conseil du 4 décembre 2001 établissant des exigences et des procédures harmonisées pour le chargement et le déchargement sûrs des vraquiers.
- Directive 2000/59/CE du Parlement européen et du Conseil du 27 novembre 2000 sur les installations de réception portuaires pour les déchets d'exploitation des navires et les résidus de cargaison.

[51] (Guidelines on Maritime Cyber Risk Management, 2017)
[52] (Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities, 2021)

5.3 Législation en matière de cybersécurité

L'UE a adopté et renforcé le code ISPS par deux directives : la directive CE/725/2004 pour les installations portuaires et la directive CE/65/2005 pour les ports. L'UE protège ses infrastructures (y compris les IIC maritimes) au moyen de divers instruments juridiques :

La *directive NIS* a établi une compétence européenne en matière de cybersécurité pour protéger le marché unique numérique ; elle a trois objectifs principaux : a) Améliorer les capacités nationales en matière de cybersécurité en exigeant de tous les États membres qu'ils disposent d'un ensemble de capacités minimales communes. C'est-à-dire des centres de réponse aux incidents de sécurité informatique (CSIRT) dotés de ressources suffisantes. b) Faciliter la coopération transfrontalière au niveau de l'UE entre les États membres et l'Union, tant au niveau stratégique/politique qu'au niveau opérationnel en matière de cybersécurité. Cela concerne à la fois le groupe de coopération NIS et le réseau des CSIRT. c) Promouvoir une culture de la gestion des risques et du signalement des incidents parmi les principaux acteurs économiques, notamment les opérateurs de services essentiels (OSE) pour le maintien des activités économiques et sociétales et les fournisseurs de services numériques (FSN).

La *législation européenne sur la cybersécurité* établit un cadre de certification de la cybersécurité pour les produits et les services. Ce cadre fournira des systèmes de certification à l'échelle européenne sous la forme d'un ensemble complet de règles, d'exigences techniques, de normes et de procédures. Il sera ainsi possible de s'assurer que le public ait confiance dans la cybersécurité des produits et services TI. Il est important de pouvoir démontrer qu'un produit a été vérifié et certifié conforme à des normes de cybersécurité élevées. Les produits liés à l'IA gagneront en confiance s'ils sont certifiés et, dans les années à venir, divers systèmes de cybersécurité seront élaborés pour les produits liés à l'IA, précisant ainsi les exigences en matière de sécurité.

Le *Règlement général sur la protection des données (RGPD)* établit des règles de protection des données des utilisateurs en détaillant les conditions dans lesquelles des tiers peuvent accéder aux informations les concernant. Le RGPD prévoit des limites sur ce que les organisations peuvent faire avec les données personnelles.

Le *Nouveau cadre législatif (NLF)* améliore la surveillance du marché, introduit des règles visant à mieux protéger les consommateurs et les professionnels contre les produits dangereux (communautaires ou non), fixe des règles pour l'accréditation et établit un cadre juridique commun pour les produits industriels. Le NLF renforcera la sécurité des produits basés sur l'IA.

Le *Règlement européen sur les semi-conducteurs* est pertinent pour la sécurité liée à l'IA, car les semi-conducteurs représentent la technologie du 21e siècle qui sera utilisée pour le développement de l'IA et pour l'intégration de mesures de sécurité solides. L'industrie européenne des semi-conducteurs sera soutenue par cette proposition de législation.

Le *Règlement sur la cyber-résilience* établira en temps utile de nouvelles règles de cybersécurité pour les produits numériques et les services auxiliaires. Cette initiative

favorisera également la sécurité des produits basés sur l'IA puisqu'elle vise à répondre aux besoins du marché et à protéger les consommateurs contre les produits non sécurisés en introduisant des règles communes de cybersécurité pour les fabricants et les vendeurs de produits numériques matériels et immatériels.

6 Bonnes pratiques dans le domaine de la sécurité maritime

6.1 Introduction

Les infrastructures critiques maritimes (ports ou navires) doivent être considérées comme des infrastructures physiques et informatiques.
Il existe plusieurs lignes directrices concernant la sûreté des infrastructures maritimes critiques :

- **Bonnes pratiques en matière de cybersécurité dans le secteur maritime publiées par l'ENISA** (2019)
- **ETSI TR 103 456** CYBER ; Mise en œuvre du NIS **COM(2017) 476 final** "Making the most of NIS" (Tirer le meilleur du NIS)
- **C(2017)6100 final** Recommandation sur la réponse coordonnée aux incidents et crises de cybersécurité de grande ampleur (plan)
- **Gestion et auto-évaluation des navires-citernes - TMSA** (OCIMF)
- **Directives sur la cybersécurité à bord des navires** (soutenues par : **BIMCO**, CLIA, **ICS**, INTERCARGO, INTERTANKO, OCIMF et IUMI)
- **Sensibilisation à la cybersécurité** - AMMITEC

Ce chapitre souligne les étapes à suivre au niveau personnel, organisationnel et opérationnel pour relever de manière globale les défis en matière de sécurité.
La sécurité est considérée comme une responsabilité commune et tous les acteurs concernés doivent adopter de bonnes pratiques en matière de cybersécurité. Deux questionnaires ont été élaborés (voir annexes A et B) et seront distribués à l'avenir aux opérateurs maritimes afin de déterminer leur niveau de sensibilisation à la sécurité.

6.2 Gouvernance de la sécurité maritime

L'hygiène en matière de sécurité d'une IC maritime (port, navire, compagnie maritime) fait partie intégrante de la structure globale de l'IC. Il s'agit de l'ensemble des mesures à prendre pour que l'IC maritime puisse fonctionner à un niveau de risque acceptable face aux menaces physiques, informatiques, hybrides et à celles qui pèsent sur la chaîne d'approvisionnement. Pour mieux comprendre l'hygiène de sécurité d'une IC maritime, il convient avant tout de savoir quelles sont les principales autorités et parties prenantes qui constituent la structure globale, participent aux opérations et aux services, mais aussi qui sont les utilisateurs internes et externes. Il est également nécessaire d'identifier toutes les installations physiques et informatiques de l'IC maritime, leurs interconnexions, leur interaction et leur importance (valeur) pour les opérations de l'IC. Un propriétaire doit être assigné à chaque installation et devra être responsable de sa sécurité (un propriétaire peut être responsable de plusieurs installations).

Une IC maritime est un système de systèmes intégré dans une seule entité. Pour mieux comprendre l'écosystème de l'IC, il est nécessaire de savoir qui s'occupe de la gestion des

installations. Ce point est important car il renseigne sur la gouvernance de la sécurité de l'information d'une IC maritime et sur les mesures de sécurité globales qui doivent être prises pour protéger ces installations.

Chaque IC maritime doit appliquer et mettre en pratique un plan de gouvernance de la sécurité de l'information, tel que précisé ci-dessous :

- Politiques (obligatoires)
- Normes (obligatoires)
- Lignes directrices (non obligatoires)
- Procédures (obligatoires)
- Lignes de base (obligatoires)

Les politiques, les normes, les lignes directrices et les procédures posent les jalons de la gouvernance de la sécurité d'une organisation. À cet égard, il est possible d'acquérir une hygiène de sécurité par l'application des éléments de la gouvernance de la sécurité et d'un SGSI bien protégé qui : (i) se base sur les contrôles de sécurité appropriés, (ii) met en œuvre les contrôles de sécurité, (iii) procède à l'évaluation des contrôles de sécurité appliqués dans l'environnement maritime, et (iv) contrôle leur efficacité à intervalles réguliers. L'hygiène de sécurité doit être appliquée sur la base de la gouvernance de la sécurité décrite ci-dessus.

La structure de gouvernance doit être appliquée aux deux aspects de la sécurité (sûreté et cybersécurité) selon une approche uniforme et doit faire partie intégrante de toutes les activités de l'IC maritime. Les procédures de gouvernance doivent inclure une analyse des incidences sur les activités (BIA), une évaluation des risques actualisée et une politique de sécurité. À cet égard, la gouvernance de la sécurité de l'information doit faire l'objet d'un suivi et d'une évaluation régulière sur la base d'indicateurs clés de performance (ICP) et d'indicateurs clés de risque (ICR) concernant la sécurité physique et la cybersécurité, ainsi que la sécurité du personnel. Une équipe de traitement des incidents doit faire partie de l'équipe de gouvernance de la sécurité, qui sera responsable de la prévision, de l'identification, de l'analyse, de l'atténuation et du rétablissement post-incident (physique, informatique, hybride).

Il convient de créer une autorité centrale chargée de superviser la mise en œuvre de la gouvernance en matière de sécurité de l'information en inspectant (contrôle de la sécurité) le système de sécurité global de l'infrastructure maritime critique.

6.3 Hygiène des opérateurs en matière de cybersécurité

Selon le Rapport d'investigations sur les violations de données (DBIR) de Verizon publié en 2019, près d'un tiers (32 %) de toutes les violations de données sont associées à des escroqueries par hameçonnage.[53] Un nouveau site d'hameçonnage est créé toutes les 20 secondes, comme l'indique le rapport 2020 « Mobile Threat Landscape Report » de Wandera. L'erreur humaine a été à l'origine de 90 % des cyber-violations de données en 2019, selon l'analyse des données de l'Information Commissioner's Office (ICO) britannique réalisée par

[53] (Widup, 2019)

CybSafe. D'après cette analyse, 90% des 2 376 cyberattaques signalées à l'ICO l'année dernière ont été causées par des erreurs imputées aux utilisateurs finaux. Les attaques de phishing représentent plus de 80 % des incidents de sécurité signalés ; 17 700 dollars sont perdus chaque minute à cause d'attaques de phishing ; 60 % des violations concernent des vulnérabilités pour lesquelles un correctif était disponible mais n'a pas été appliqué par les administrateurs.

Les bonnes pratiques en matière de sécurité personnelle doivent être appliquées par tous les opérateurs maritimes et les utilisateurs individuels en établissant des règles et en s'efforçant de :

- Bâtir une culture de la sécurité et de l'hygiène informatique
- Encourager le partage d'informations et la collaboration
- Impliquer les opérateurs et les utilisateurs dans les décisions et les procédures liées à la sécurité
- Utiliser des affiches et des rappels
- Organiser une formation pratique continue en matière de sécurité à tous les niveaux (des séminaires aux exercices)
- Contrôler efficacement les accès
- Appliquer des politiques d'authentification et de mot de passe

6.4 Gestion de la sécurité maritime

La gestion des risques physiques, informatiques et hybrides nécessite une approche globale. Les mesures générales à prendre lors de la gestion de la sécurité (sûreté et cybersécurité) d'une IC maritime sont les suivantes :

1) Identifier les installations (physiques et informatiques) et y attribuer un propriétaire, en désignant, par exemple, une ou plusieurs personnes qui seront responsables de l'installation.
2) Créer un inventaire dynamique et actualisé des installations (liste des propriétaires).
3) Catégoriser et classer les installations sur la base des éléments suivants :
   - Valeur de l'installation (importance pour l'IC maritime) ;
   - Importance de l'installation dans l'écosystème maritime global ;
   - Type d'installation (physique, informatique, utilisateur, procédures).
4) Identifier l'ensemble des menaces et la surface d'attaque de chaque installation.
5) Sélectionner et utiliser une méthodologie d'évaluation des risques (par ex., à partir de l'inventaire de l'ENISA)[54] et faire une estimation des risques.
6) Prendre des mesures pour protéger les installations en utilisant des listes de contrôles publiées (ISO 27002, NIST2020, SANS Top 20, CIS), les meilleures pratiques, et élaborer un plan de traitement des risques (plan d'urgence).
7) Élaborer une politique de sécurité avec des règles qui régissent la gestion, la protection et la distribution des installations au sein de l'organisation, en s'appuyant

[54] (Inventory of Risk Management / Risk Assessment Methods and Tools , n.d.)

sur les efforts existants (le code ISPS, les lignes directrices du BIMCO ou la norme ISO/IEC PDTR 13335-1 (11/2001)).

8) Identifier en permanence les nouvelles menaces et les nouveaux incidents, évaluer les risques, les responsables des installations de l'IIC, la solidité des contrôles et la gestion des incidents.

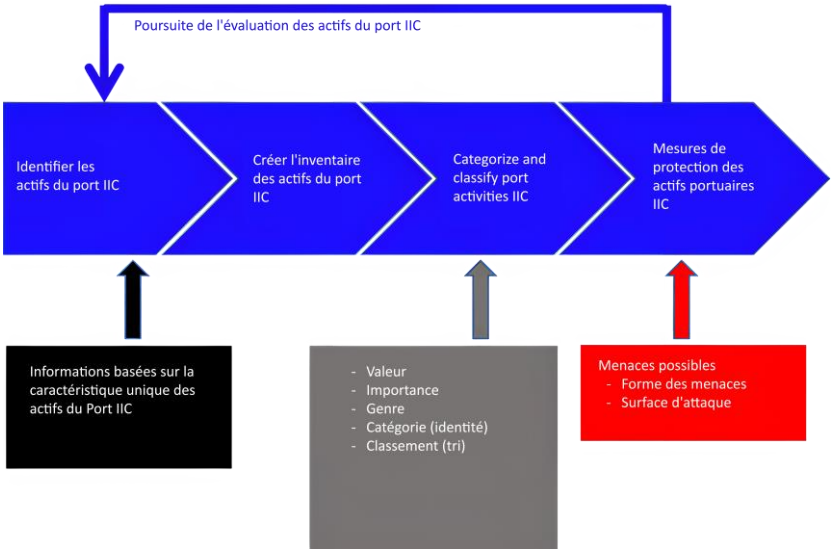


Image 9: Approche de la gestion de la sécurité par le BIMCO

6.4.1 Gestion de la sûreté (sécurité physique)

Avant la catastrophe du 11 septembre, les navires marchands entraient habituellement dans les eaux territoriales et les ports sans inspection, afin de faciliter la fluidité des échanges économiques et d'éviter de retarder les navires. Ce n'est que lorsque le navire était au mouillage ou amarré que les autorités portuaires, les douanes et les services d'immigration montaient à bord pour inspecter le navire, l'équipage et la cargaison. Cette situation rendait le port très vulnérable aux attaques des organisations criminelles et terroristes. Une attaque terroriste contre un port pourrait avoir de graves répercussions sur les populations locales, les infrastructures portuaires et les économies régionales qui dépendent de ces activités.

Les règles et protocoles de gestion de la sûreté portuaire contribuent également à prévenir les accidents et donc à réduire la gravité des blessures le cas échéant. Ces paramètres sont essentiels car ils créent un environnement de travail exempt de dangers et à faibles risques. Cette pratique améliore la qualité des opérations du terminal, la réputation du port et peut être considérée comme un outil commercial pour attirer davantage de navires.

L'OMI a été choisie comme l'organisation idoine pour élaborer un nouveau code de sécurité. Ce dernier est entré en vigueur le 1er juillet 2004, le code ISPS. Initialement axé sur la gestion de la sécurité physique (sûreté), il met désormais de plus en plus l'accent sur les risques liés à la cybersécurité et, à l'avenir, il se concentrera sur les risques aériens (c'est-à-dire les attaques de drones).

Dans certains ports maritimes, cependant, des problèmes de sûreté subsistent. Ainsi, le port et ses installations restent la cible de menaces potentielles. Cela s'explique en partie par le fait que le code ISPS transposé dans la législation nationale traite seulement des mesures de sûreté à prendre dans les installations portuaires et non dans la zone portuaire autour de ces terminaux ou dans les installations des partenaires commerciaux de la chaîne d'approvisionnement des ports.

Un port maritime est un centre logistique et industriel dans la chaîne d'approvisionnement économique mondiale. Les activités portuaires telles que le stockage et la manutention des navires sont directement ou indirectement liées au transport international et aux processus d'information, lesquels s'appuient sur de nombreux acteurs. Cela signifie que de nombreuses personnes entrent et sortent des ports par des navires, des camions, des trains, des véhicules ou en tant que piétons. Le COP et le code ISPS exigent que tous ces mouvements soient contrôlés afin de prévenir les actes illégaux. L'objectif de cette section n'est pas d'expliquer le code ISPS dans son intégralité ou tous les détails du code de bonne pratique sur la sûreté dans les ports, mais de comprendre comment ces codes peuvent être appliqués dans les ports pour mieux résister aux attaques. Toutes les mesures de sécurité et les pratiques opérationnelles quotidiennes ci-dessous sont décrites plus en détail dans le PSP et le PFSP.

6.4.1.1 Limites du port et de l'installation portuaire

Les deux codes exigent que toutes les personnes soient contrôlées à l'entrée et à la sortie du port ou d'une installation portuaire. Mais quelles sont les limites administratives de l'infrastructure et, surtout, celles du port à surveiller ?

Les observations montrent que dans certains cas, les capitaines de port ne savent pas s'ils doivent être tenus pour responsable, en tant qu'autorité portuaire, en cas d'incidents survenus à 90 milles en mer, dans la baie du port ou sur une plage voisine située en dehors de la zone portuaire visible. Nous avons observé qu'il y avait une certaine incompréhension entre l'autorité portuaire et les opérateurs de terminaux privés quant à l'entité à qui la responsabilité des incidents qui se produisent dans le bassin devant l'installation portuaire concernée était imputable. Il est important d'inclure les limites administratives exactes du port et de chaque installation portuaire (y compris les limites des eaux) dans le plan de sûreté portuaire (PSP) et le plan de sûreté de l'installation portuaire (PFSP). Cela permet de prendre les mesures les plus efficaces et de contacter les bonnes personnes en cas d'urgence. Des actions efficaces permettent de prévenir les dommages et d'assurer un rétablissement rapide des conditions économiques normales.

6.4.1.2 Responsabilité en matière de sécurité

Les installations portuaires sont responsables en dernier ressort de la gestion des incidents liés à la sûreté au titre du code ISPS. Cela signifie que l'agent de sûreté de l'installation portuaire (PFSO) doit agir conformément au code ISPS et que l'agent de sûreté portuaire (PSO) doit agir conformément aux lignes directrices du COP. Il n'appartient pas au PSO d'assumer la responsabilité globale des risques survenant dans les installations portuaires, mais de coopérer avec le PFSO le cas échéant.

L'expérience montre que dans certains pays, le code ISPS a été transposé dans la législation nationale en tant que loi sur la sécurité, et désigne le PSO comme ultime responsable en cas d'incidents de sécurité. Cela place le PSO dans une situation où le port (plutôt que l'installation portuaire) devient l'ultime responsable des incidents de sécurité au titre du code ISPS dans les installations portuaires. Il en résulte que les risques de sécurité ne sont pas résolus, car il est peu probable que le port investisse dans des mesures de sécurité dans le cadre d'une concession d'installation portuaire privée.

6.4.1.3 Le système de gestion de la sécurité (SeMS)

Pour faire preuve d'une gouvernance adéquate, les départements de sécurité portuaire doivent être bien organisés et prendre en compte les menaces physiques et informatiques. Ils doivent être en mesure de contrôler et de corriger les activités de sécurité quotidiennes. Pour ce faire, ils ont besoin d'outils de gestion. Grâce à un système de gestion, ils peuvent contrôler l'état de l'infrastructure de sécurité, les performances du personnel de sécurité et vérifier que toutes les fonctions de sécurité sont correctement exécutées.

Dans de nombreux ports, aucun SeMS n'est disponible. Les agents de sécurité agissent parfois comme des gestionnaires de crise et se concentrent sur l'atténuation des incidents plutôt que sur leur prévention. Ils devraient gérer tous les aspects de la sécurité et prendre des mesures quotidiennes pour prévenir les incidents physiques, informatiques et hybrides. Le système de gestion de la sécurité de l'information (SGSI), qui fait partie du SeMS, est mis en œuvre conformément aux exigences de la norme ISO 27001.[55] Toutes les infrastructures critiques du port doivent répondre aux exigences de la norme IS0 27001 et gérer les cyber-risques.

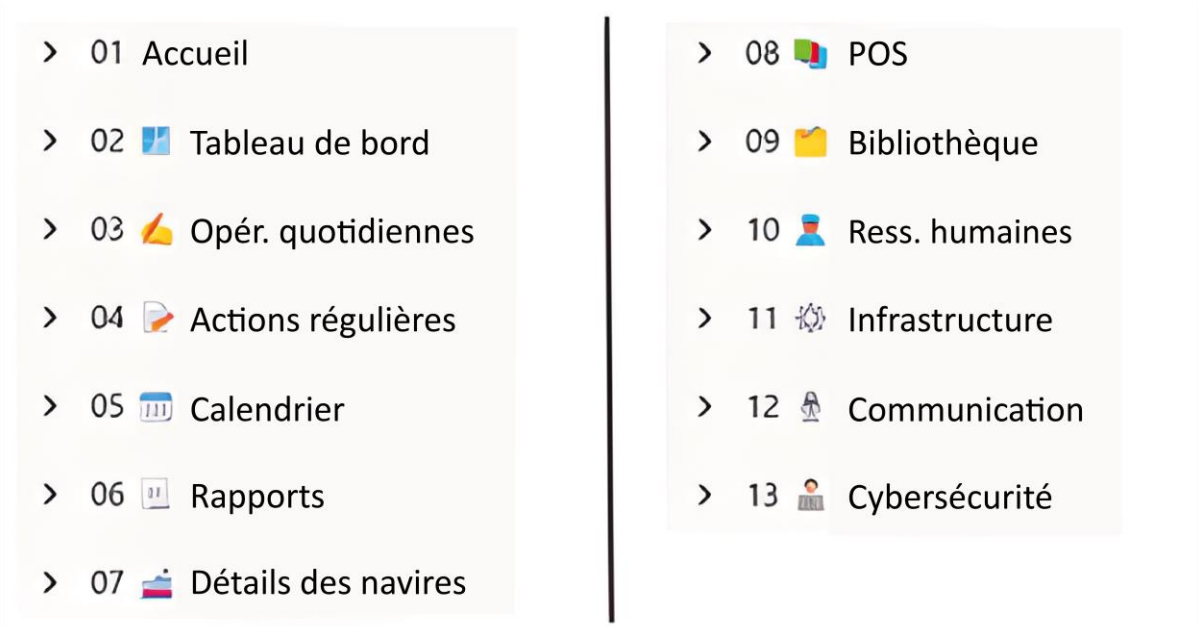


Image : Exemple de SeMS (Christophe Van Maele)

[55] (ISO/IEC 27001 and related standards: Information security management, n.d.)

6.4.1.4 Contrôle de sécurité physique aux portes

Chaque fois qu'une personne (à pied ou en véhicule) entre dans une infrastructure ISPS, sa carte d'identification (ou son badge) doit être vérifiée avant d'être admise dans la zone. Le code exige un enregistrement de la personne et de l'heure d'entrée. Lorsque la personne quitte une infrastructure ISPS, l'heure de son départ doit être enregistrée. Cela permet de savoir qui se trouve dans une zone ISPS à tout moment, et peut faciliter la recherche d'une personne spécifique à un moment donné ou lors d'une évacuation d'urgence. La technologie peut être d'une grande aide, car les barrières électroniques, les tourniquets et les systèmes de badges numériques permettent de se débarrasser des erreurs liées aux enregistrements manuels, surtout si l'établissement compte plusieurs entrées et sorties.

La réalité montre que l'enregistrement manuel est encore la norme dans de nombreux ports. En outre, les barrières manuelles permettent d'entrer en passant par un gardien. Ce dernier décide seul d'autoriser ou non l'accès sans que sa décision ne fasse l'objet d'une vérification.

Si le port est le premier point d'entrée, ce qui est souvent le cas lorsque la zone portuaire est une zone de libre-échange, les mêmes principes de contrôle de sécurité doivent être appliqués. Là encore, de nombreuses lacunes sont constatées dans la pratique.

6.4.1.5 Contrôle de sécurité dans la zone portuaire

Des agents de sécurité mobiles effectuent des patrouilles et vérifient que les personnes sont autorisées à pénétrer dans la zone ISPS ou dans la zone portuaire. Pour faciliter cette tâche, toute personne se trouvant dans la zone doit porter un badge d'identification de façon visible. Toutefois, les contrôles d'identité sont rarement effectués et toutes les personnes ne portent leur badge de manière ostentatoire.

6.4.1.6 Contrôle de la sécurité du périmètre

Il s'agit du contrôle des limites administratives du port ou de l'installation portuaire. Dans la plupart des cas, il s'agit de barrières physiques mais au sein de l'Union européenne certains terminaux non critiques, tels que les terminaux manipulant du sable, ne sont pas tenus d'être clôturés. Ils disposent parfois d'un système de caméras pour surveiller les limites de la zone. La surveillance du périmètre est souvent effectuée à partir d'un centre de contrôle de sécurité où les opérateurs analysent les images et décident des mesures à prendre. Leurs collègues des équipes mobiles de surveillance effectuent des rondes de sécurité. Une bonne pratique consiste à utiliser un système de ronde balisée pour s'assurer qu'ils ont vérifié toutes les zones marquées par des balises. Les rondes balisées ne sont parfois pas effectuées. Les opérateurs pourraient être mieux formés à cette pratique dans de nombreux ports.

6.4.1.7 Communication entre tous les responsables de sécurité

Des réunions régulières devraient être organisées entre les PFSO et les PSO pour s'informer de manière détaillée de la sécurité dans le port, discuter des risques potentiels, gérer les incidents et se tenir au courant des nouveaux événements dans le port. Les PSO devraient organiser le même type de réunions au niveau national (Comité national de sécurité maritime) avec d'autres parties prenantes telles que la police portuaire, les douanes, la marine, les autorités compétentes, etc. Lors de ces réunions, il serait possible de discuter des

questions de sécurité d'intérêt national et d'aborder les cas de situation grave, comme le passage au niveau de sûreté 2 ou 3.

Dans certains pays, les différentes parties prenantes restent sur leur propre terrain et ne se rencontrent pas régulièrement, voire pas du tout. Dans ce cas, il n'existe souvent pas de plan d'action coordonné ou bien il n'existe que sur papier. Les activités criminelles ne sont ainsi pas détectées.

6.4.1.8 Renforcement des capacités par la formation du personnel

Il est essentiel de disposer d'un personnel de sécurité bien formé, qui sait comment faire son travail. Les personnes travaillant dans les ports changent parfois d'emploi. Il est donc nécessaire d'organiser régulièrement des sessions de formation pour les nouvelles recrues et des exercices pour le personnel de sécurité. Outre la formation ISPS de base, la formation sur le terrain est tout aussi importante pour comprendre comment manipuler les applications numériques de la salle de contrôle et comment agir en cas d'urgence.

Les formations sont considérées comme nécessaires dans tous les ports du monde. Il est important de maintenir des normes de formation élevées afin d'éviter que le personnel formé ne soit pas en mesure de répondre efficacement aux incidents.

6.4.1.9 Gestion des incidents de sécurité

Une fois que le port a mis en œuvre des principes appropriés de gestion de la sécurité, les installations portuaires conformes à l'ISPS peuvent être considérées comme protégées contre les actions illégales et intentionnelles. Il s'agit notamment des principes préventifs susmentionnés visant à protéger les personnes contre le vol, le vandalisme, le terrorisme, les cyberattaques, la violence, le trafic de drogue et d'autres menaces. Il est important de comprendre que, tant dans la réglementation que dans la gestion quotidienne, l'ISPS et le COP sont basées sur la prévention. Cela signifie que les mesures de sécurité portuaire sont prises pour anticiper les menaces potentielles avant qu'elles ne se produisent. Ces mesures visent à dissuader les criminels et à réduire la probabilité qu'un délit grave ou qu'un acte de violence ne soit commis. Les évaluations obligatoires de sécurité en vertu du code ISPS (Processus d'évaluation de la sûreté (PSA)/ Évaluation de la sûreté de l'installation du port (PFSA)) et les plans de sûreté (PSP / PFSP) constituent la base de la conformité.

En cas d'incident de sécurité, le rôle du port peut changer. Le passage à un niveau de sûreté ISPS supérieur relève de la décision de l'autorité compétente. Dans ce cas, une équipe stratégique de gestion de crise est constituée et les forces de l'ordre sont appelées pour faire face à la situation grave. Ainsi, le port ne décide généralement pas lui-même des mesures de sécurité proactives et immédiates à prendre. Les mesures à long terme sont proposées par le port (l'infrastructure), approuvées par l'autorité compétente et incluses dans le plan de sûreté du port (l'infrastructure). Ce n'est que par la suite qu'elles sont mises en œuvre.

Les systèmes TI et TO sont également utilisés en permanence. Dans le domaine de la sécurité des ports et des terminaux conformes à l'ISPS, il est nécessaire de prendre en compte les éléments suivants :

- le système de gestion de la sécurité n'est efficace que s'il est numérisé

- le système de badges d'identification est efficace lorsqu'il s'agit d'un système numérique s'appuyant sur une base de données commune à laquelle les forces de l'ordre et les douanes ont également accès
- le système de barrière automatique n'admet que les personnes autorisées à entrer dans la zone
- un système de surveillance du périmètre doté d'un système de vidéosurveillance ou d'un autre système de caméras très performant prendra des mesures intelligentes et pourra suivre les séquences vidéo pendant de longues périodes.
- l'utilisation d'ordinateurs pour communiquer entre les parties prenantes permet de prendre des mesures efficaces en temps réel lorsque cela est nécessaire. Les systèmes d'information relèvent néanmoins de la compétence du département informatique

À ce jour, plusieurs de ces systèmes de sécurité n'ont pas été installés dans les ports couverts par l'étude. Par conséquent, les systèmes de ces ports ne pourraient pas être attaqués par des cyber-terroristes. Ce type de risque ne se produira que lorsque les systèmes de sécurité de ces ports seront numérisés.

6.4.1.10 Contrôle des systèmes d'information

Étant donné que les opérations de sécurité quotidiennes sont de plus en plus numérisées, un grand nombre d'informations ont besoin d'être partagées et protégées. Ce point est décrit plus en détail dans le chapitre sur la cybersécurité.

6.4.1.11 Gestion de la sécurité des navires

Le code ISPS s'applique aux installations portuaires et aux navires. Bien que le même code s'applique aux deux zones, certains aspects ne s'appliquent qu'à bord d'un navire. Si un terroriste prend le contrôle d'un navire, de sa cargaison, de son équipage et de son système d'information, il peut paralyser un port pendant une longue période. L'agent de sûreté du navire (SSO) est responsable de la bonne gestion de la sûreté à bord, conformément au code ISPS, afin de prévenir les attaques de pirates et les détournements de navires. Ils sont supervisés par leur agent de sûreté de la compagnie (CSO). Les principes de gestion correspondent à ceux qui s'appliquent au port.

Afin de se préparer aux menaces extérieures, l'OMI a pris l'initiative d'aider les navires en leur fournissant des directives pour prévenir les attaques. Un navire doit être capable de résister à une attaque extérieure grâce à des directives en matière de protection des navires. La mise en œuvre de ces mesures de protection est divisée en trois niveaux : un premier niveau de défense, un deuxième niveau de protection et une couche finale.

- Le premier niveau de défense protège le navire contre l'abordage par des attaquants. Parmi les composantes, on retrouve des équipes de surveillance vigilantes, des projecteurs, des manœuvres pour éloigner le navire des attaquants, des fils barbelés et des arroseurs et, dans certains cas, des gardes armés sous contrat.
- Le deuxième niveau de défense intervient une fois les assaillants à bord et vise à protéger le pont et l'accès au château. Cela peut se faire par le biais de verrous, de détecteurs de mouvement, de systèmes de vidéosurveillance et d'une équipe vigilante.

- Le troisième niveau de défense s'active si les attaquants prennent le contrôle du pont et accèdent au système d'information. Dans ce cas, l'équipage peut se cacher dans un bunker spécialement conçu à cet effet, appelé « citadelle », où il est possible d'accéder aux commandes vitales du moteur et de la barre, et où le système de communication peut être surveillé.

L'équipage doit avoir une maîtrise parfaite du fonctionnement de l'équipement de la citadelle et connaître les moyens à sa disposition pour conserver le contrôle du navire dans ce cas de figure. S'ils ne sont pas correctement formés pour contrôler le navire à partir de ce bunker, la citadelle elle-même peut devenir une prison mortelle pour l'équipage qui s'y est réfugié pour sa propre protection.

6.4.2 Gestion de la cybersécurité

Le modèle de gestion de la cybersécurité mis au point par le BIMCO[56] (sur la base du Cadre de gestion des risques (RMF) du NIST)[57] suit les principales étapes de l'évaluation de la sécurité décrites à la section 6.4 et contient les éléments suivants concernant la gestion de risques informatiques :

1. Identifier les menaces
2. Identifier les vulnérabilités
3. Évaluer l'exposition au risque (estimation du risque)
4. Développer des mesures de détection et de protection
5. Établir des plans d'urgence
6. Répondre aux incidents de cybersécurité et garantir un retour à la normale

Le point le plus important en matière de cybersécurité est d'identifier l'ensemble des menaces, ce qui signifie concrètement qu'il est nécessaire de déterminer quelles sont les menaces potentielles susceptibles d'affecter les installations de l'IC maritimes. Voici quelques exemples de cybermenaces identifiées en 2020 par l'ENISA[58]: (1) logiciels malveillants, (2) attaques sur Internet (3) hameçonnage, (4) attaques d'applications web, (5) spam, (6) DDoS, (7) usurpation d'identité, (8) violation de données, (9) menace interne, (10) réseaux zombies, (11) manipulation physique, endommagements, vol et perte, (12) fuite d'informations, (13) ransomware, (14) cyberespionnage, (15) minage de cryptomonnaie malveillant.

Une fois que l'ensemble des menaces est identifié, la surface d'attaque (l'ensemble des attaques qui peuvent être utilisées pour exploiter les failles) des installations de l'IC peut être facilement identifiée (point 4 du paragraphe 6.4 ci-dessus). La surface d'attaque de ces installations peut être déterminée en fonction de leurs vulnérabilités. Il est donc nécessaire de procéder à une évaluation de ces dernières.

L'étape suivante définie par le BIMCO consiste à évaluer l'exposition au risque concernant les

[56] (The Guidelines on Cyber Security onboard Ships - Version 4, 2020)
[57] (NIST Risk Management Framework (RMF), n.d.)
[58] (European Union Agency for Cybersecurity (ENISA), 2020)

installations de l'IC. En outre, le risque est divisé en quatre types de réponse, à savoir :

- *éviter le risque*: dans ce cas, le risque n'est pas accepté (une décision de la direction du port doit être prise sur recommandation du responsable de la sécurité des systèmes d'information (RSSI)).
- *transférer le risque* (par ex., à une compagnie d'assurance) : une décision de la direction du port doit également être prise sur recommandation du RSSI car elle peut avoir un impact financier.
- *prendre des mesures d'atténuation* : l'atténuation du risque est également une décision qui doit être prise par la direction du port sur recommandation du RSSI, car elle peut également avoir un impact financier.
- *risque accepté*: l'acceptation du risque est une décision commerciale directe et seule la direction peut en prendre l'initiative.

Pour atténuer le risque, des mesures de protection et de détection doivent être élaborées et un plan d'intervention doit être établi pour ramener le risque à un niveau acceptable. Le niveau acceptable est défini par l'IC maritime (**appétit pour le risque**) après avoir effectué une analyse coût-bénéfice ou après avoir identifié l'impact du risque sur l'activité. La **matrice de l'appétit pour le risque** décrit une analyse qualitative du risque :

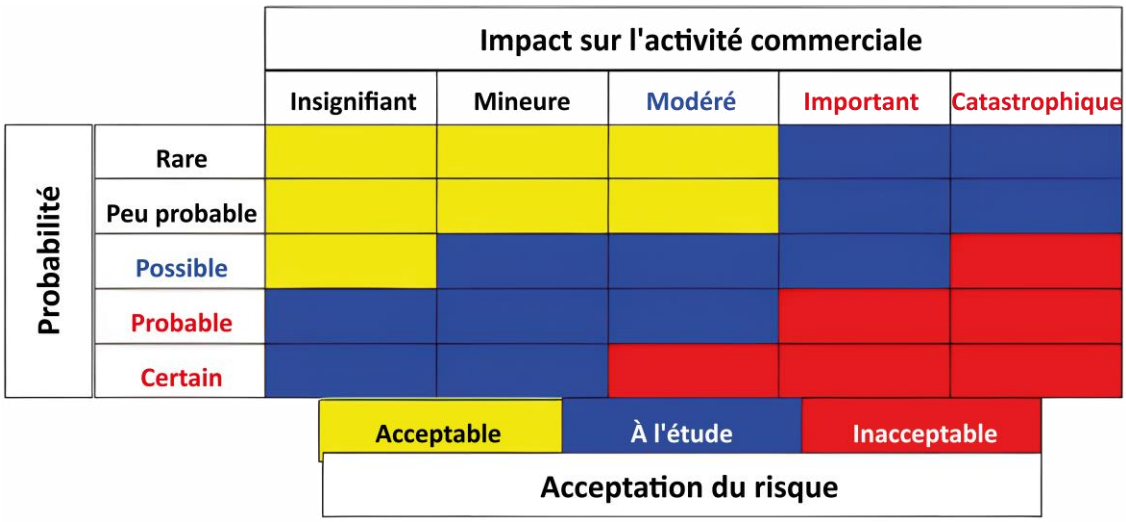


Image 10**:** Matrice de l'appétit pour le risque

Si les mesures d'atténuation ne permettent pas de ramener le risque à un niveau acceptable selon la matrice, une décision commerciale doit être prise par la direction du port afin d'accepter ou non le risque.

Les risques doivent être évalués au cas par cas en fonction de l'écosystème informatique de l'IC et doivent donc être définis comme (i) risques acceptables (ii) risques à examiner (mesures d'atténuation ou transfert de risques) (iii) risques inacceptables, à éviter.

Les lignes directrices du BIMCO sur la cybersécurité à bord des navires reposent sur des principes de haut niveau :

- la sensibilisation aux risques en matière de sécurité et de sûreté, mais également aux risques économiques qui découlent de l'absence de mesures de cybersécurité ;
- la protection de l'infrastructure TI de bord et des équipements connectés ;
- présence d'un système d'authentification et d'autorisation des utilisateurs, afin de garantir un accès approprié aux informations nécessaires ;
- la protection des données utilisées dans l'environnement du navire, en veillant à ce qu'elles bénéficient d'une protection adéquate en fonction de la sensibilité de l'information.

Image 11: Approche du BIMCO au sujet de la gestion de la cybersécurité[59]

- la gestion des utilisateurs de technologies de l'information, afin de s'assurer qu'ils n'ont accès et ne disposent de droits que pour les informations pour lesquelles ils sont habilités ;
- la gestion de la communication entre le navire et le continent, et
- l'élaboration et la mise en œuvre d'un plan d'intervention en cas d'incident informatique sur la base d'une évaluation des risques.

La valeur des installations du port (importance dans les opérations maritimes) détermine les exigences de sécurité et les contrôles à effectuer. Divers efforts (dont le projet SAURON) contribuent à la classification des installations portuaires et proposent des architectures de sécurité.

[59] (Lignes directrices sur la cybersécurité à bord des navires - Version 4, 2020)

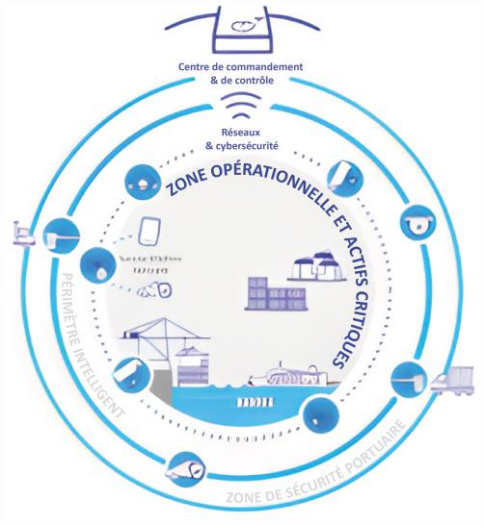


Image 12: Architecture de sécurité physique et informatique SAURON[60]

Cette approche contribue à la sécurité des ports en assurant la sécurité des installations physiques et des installations informatiques.

6.5 La cyber-résilience maritime

La cyber-résilience maritime[61] est la capacité de l'IC maritime à résister aux attaques. La résilience est atteinte si la sécurité (sûreté et cybersécurité) est assurée et si la structure de gouvernance est efficace et vérifiable. Par exemple, si la robustesse des contrôles et des procédures de sécurité (telles que les procédures de reprise après sinistre) est régulièrement testée.

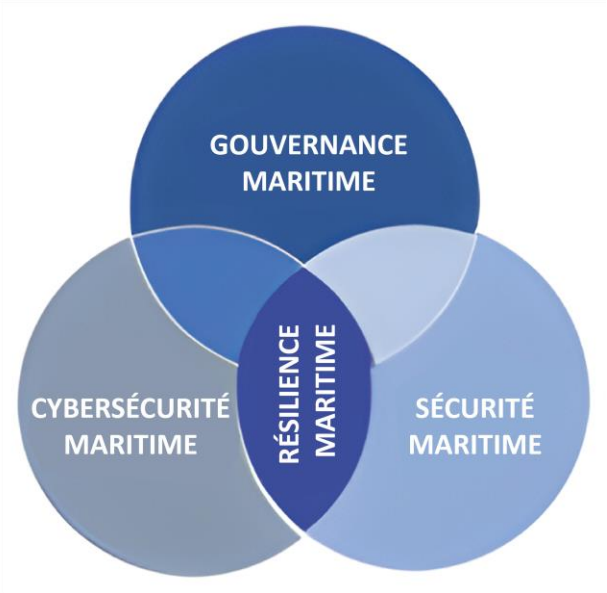


Image 13: Résilience maritime

[60] (Company, 2017); (Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports, n.d.)
[61] (Erstad, Ostnes, & Lund, 2021)

Diverses organisations adoptent une vision plus générale de la sécurité. A titre d'exemple, selon l'Institution of Engineering and Technology (IET),[62] la sécurité s'efforce d'atteindre et de maintenir huit objectifs généraux, comme indiqué ci-dessous :

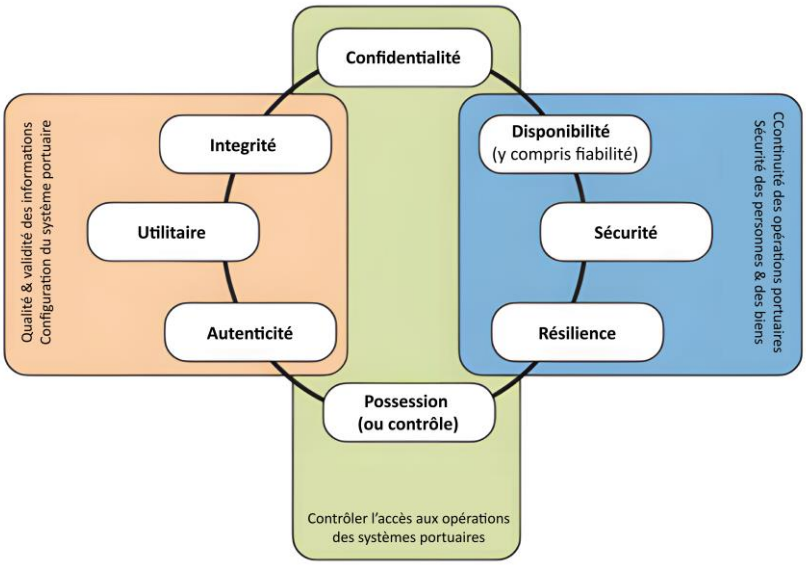


Image 14: Objectifs de sécurité de l'IET

6.6 Facteurs humains

La nature humaine, le comportement, les valeurs sociales, culturelles et morales font de l'individu à la fois le principal catalyseur des cyberattaques, un défenseur compétent en matière de cybersécurité, un opérateur et un officier maritime rompu à la sécurité. Les profils humains et leurs caractéristiques jouent un rôle majeur dans les progrès futurs en matière de sécurisation des installations et infrastructures maritimes.

L'étude des facteurs et paramètres humains des membres des équipes de sécurité des ports et des navires ou l'étude des profils des attaquants (à partir d'incidents de sécurité antérieurs) permet d'anticiper ou de prévenir un incident et de gérer plus efficacement une attaque.

En outre, en identifiant les profils du personnel maritime (opérateurs, agents, administrateurs, membres d'équipage, etc.), l'IC maritime pourrait mettre au point une formation à la sécurité plus efficace, centrée sur leurs besoins et leur niveau de compréhension de la sécurité. Les plans et procédures de sécurité doivent être clairs pour tous les employés afin qu'ils puissent les utiliser et s'y conformer quotidiennement[63].

[62] (Good Practice Guide: Cyber Security for Ports and Port Systems, 2020)
[63] (Kioskli & Polemi, Psychosocial Approach to Cyber Threat Intelligence, 2020); (Kioskli & Polemi, A Socio-Technical Approach to Cyber-Risk Assessment, 2020)

L'élaboration de procédures de sécurité applicables nécessite de faire participer les employés dans l'élaboration de ces procédures.

Le facteur humain est le pivot de la sécurité globale de l'écosystème maritime. En général, les ports et les navires sont les maillons les plus faibles de la chaîne de sécurité, ce qui peut entraîner une compromission des opérations et des services maritimes. Malgré les moyens technologiques mis en place, ce sont les individus qui représentent la plus grande menace.

La sensibilisation des acteurs maritimes à la sécurité doit faire l'objet d'un suivi permanent ; la distribution et l'analyse des questionnaires figurant en annexe peuvent contribuer à répondre à ce besoin. Les campagnes de sensibilisation et les formations pratiques ciblées constituent les meilleurs moyens de préparer les employés et les parties prenantes du secteur maritime à devenir les principaux garants de la sécurité contre les attaques physiques et informatiques dans l'écosystème maritime, et de renforcer la culture de la sécurité dans ce domaine.

7 Pratiques de sécurité portuaire en Afrique

7.1 Les ports du Golfe de Guinée

Tous les jours, environ 1 500 navires (pétroliers, cargos et bateaux de pêche) naviguent dans les eaux du Golfe de Guinée et accostent dans 20 ports principaux. Cet important flux économique constitue un terreau fertile pour la piraterie, l'enlèvement de marins, les vols à main armée en mer, la pêche illégale, la contrebande et le trafic d'êtres humains à l'intérieur et autour des ports. Cette situation favorise également la criminalité transnationale organisée et les attaques terroristes. C'est une menace majeure pour la sécurité maritime de tous les navires qui fréquentent ces ports et, en fin de compte, pour le développement économique des pays de toute la région.

Le potentiel économique de la région du Golfe de Guinée devrait encore s'accroître dans les années à venir, mais avant qu'elle ne puisse réaliser et bénéficier de ce potentiel, il convient d'abord de s'attaquer aux menaces qui pèsent sur sa stabilité et sa prospérité. Pour ce faire, il est nécessaire d'identifier et de relever en permanence les défis en matière de sécurité liés à la mer, aux ports maritimes et à l'arrière-pays.

Image 15: Région maritime du Golfe de Guinée[64]

7.2 Organisation de la sécurité portuaire en Afrique

Les ports maritimes d'Afrique sont organisés de la même manière que les autres ports du monde. L'autorité portuaire est gérée au quotidien par des fonctionnaires de l'État, qui sont responsables devant leurs ministères respectifs.

Une autorité portuaire compte plusieurs départements. Parmi ceux-ci, on retrouve le département informatique et le département des opérations, qui est dirigé par le capitaine du port. Les observations faites dans les ports du monde entier ont montré que le capitaine de port est désigné comme le principal responsable, en dehors des opérations nautiques, de

[64] (Gulf of Guinea Map, 2021)

la sécurité dans le port et dans les infrastructures exploitées par le port lui-même. Le service de sécurité doit mettre en œuvre les règles ISPS dans le port et appliquer le bouclier de sécurité. Le service de sécurité du port, quant à lui, se concentre sur la sécurité des individus et dispose presque toujours d'une équipe d'intervention prête à passer à l'action en cas d'incendie et de situation nécessitant l'administration des premiers soins. Au niveau administratif, le service informatique du port fournit des règles de cybersécurité relatives aux systèmes administratifs généraux du port. Toutefois, l'infrastructure de sécurité ISPS n'entre pas souvent dans son champ d'action. Elle est gérée par les sociétés externes qui ont installé le matériel de sécurité. Les ports perçoivent des revenus basés sur le volume de fret des navires de leurs clients par le biais de la « surtaxe ISPS ». Cette redevance couvre le coût de l'ensemble des mesures visant à améliorer la sécurité des installations portuaires en vertu du code ISPS.

L'architecture informatique suivante est un exemple de bonne pratique en matière de sécurité :

Il existe quatre principaux systèmes de sécurité TO et TI qui sont essentiels pour prévenir un incident de sécurité. Si l'un de ces systèmes fait l'objet d'une cyberattaque, l'intégrité de la sécurité physique du port est compromise.

- Le premier système est le *système TO de contrôle de badges* : Un système de badges s'appuie sur une base de données numérique des personnes qui ont une activité commerciale dans le port. La base de données comprend le personnel du port, les dockers, les camionneurs, les clients et les visiteurs. Après un premier contrôle administratif de la personne (par la police) lors de la demande de badge, cette dernière est autorisée à entrer dans le port certains jours et à certaines heures. Dans le meilleur des cas, la base de données est vérifiée régulièrement par la police, qui peut bloquer les personnes ayant des intentions malveillantes. Un système de badges devra être installé par une société de sécurité externe, qui dispose de droits d'administration pour maintenir le système TO. Le personnel de sécurité du port produit et distribue les badges. Si le système de badges est piraté et que le temps d'accès est prolongé, un criminel peut recevoir un badge d'accès au port et entrer dans la zone portuaire sans être détecté.
- Le deuxième système est le *système TO de contrôle d'accès* : Ce système permet aux personnes d'entrer dans les locaux du port (et de l'infrastructure portuaire) lorsqu'elles présentent leur badge dans les plages horaire autorisées. Ce système de contrôle accède à la base de données des badges et décide d'ouvrir ou non les portails, les portes, les tourniquets, les barrières d'accès, etc. Ce genre de système est généralement installé par la même société d'intégration de système de sécurité que celui des badges. Si le programme de détection du système de contrôle d'accès peut être détourné par une cyberattaque, les criminels (et leurs produits de contrebande) peuvent entrer et sortir librement du port.
- Le troisième système est le *système TO de contrôle du périmètre* : Pour contrôler le périmètre du port, il est nécessaire d'installer des clôtures et un système de surveillance pour contrôler les entrées illégales. De nos jours, des systèmes de vidéosurveillance ainsi que des systèmes de caméras thermiques et infrarouges sont utilisés dans les ports civils et les installations portuaires pour vérifier l'intégrité de la

clôture. En outre, une salle de contrôle de sécurité doit être mise sur pied pour surveiller et agir en cas d'intrusion et d'infraction. Ces systèmes de caméras sont installés par des sociétés externes spécialisées qui disposent de droits d'administration sur le système. Les caméras sont utilisées par le personnel de sécurité du port. Si le système de caméras venait à être piraté lors d'une cyberattaque, les gardes pourraient être induits en erreur et se voir présenter de fausses images, ce qui permettrait aux assaillants d'entrer illégalement ou de commettre un vol à l'intérieur du périmètre surveillé.

Image 16: Système TO de contrôle du périmètre[65]

- Le quatrième système est le *système TI* : Le système informatique utilisé par le personnel de sécurité se compose principalement d'un système de gestion de la sécurité (SeMS), de documents numériques, de courrier électronique et d'une connexion Internet. Ce système est installé par le service informatique du port, qui conserve le contrôle administratif du bouclier de cybersécurité. Si les opérateurs venaient à être victime d'une cyberattaque, par l'utilisation d'une clé USB infectée par exemple, la communication entre les agents de sécurité pourrait être entravée, ce qui entraînerait une situation dans laquelle les opérateurs de sécurité seraient aveugles.

Les autres ports d'Afrique du Sud et de l'Est appliquent les mêmes principes de sécurité que dans les ports du Golfe de Guinée. Les opérateurs portuaires privés qui détiennent des infrastructures portuaires sous concession s'organisent pour être prêts en termes de sécurité, et conformes au code ISPS.

Les autorités portuaires se concentrent sur le maintien de la sécurité de la zone portuaire commune à l'intérieur des limites administratives du port. Ils prennent des mesures pour protéger cette zone depuis les zones de mouillage et d'amarrage jusqu'aux quais des ports et à l'ensemble de la zone portuaire (zones privées exclusives).

7.3 Initiatives internationales pour les ports africains

Plusieurs projets sont axés principalement sur l'amélioration de la sécurité en haute mer, la piraterie, les actions transfrontalières et la lutte contre les stupéfiants :

[65] Photo prise par Christophe Van Maele

- Les États-Unis sont présents avec leur programme de Commandement militaire pour l'Afrique (AFRICOM). Il se concentre sur les initiatives de sécurisation des hautes mers par des navires de guerre et sur le soutien aux marines locales.
- Les pays du Golfe de Guinée et des environs ont signé le « Code de conduite relatif à la répression des actes de piraterie, des vols à main armée à l'encontre des navires et des activités maritimes illicites en Afrique de l'Ouest et du Centre » (Code de conduite de Yaoundé). Cette architecture de Yaoundé favorise la coopération maritime régionale et garantit le maintien d'un environnement maritime stable.
- L'Europe est présente avec le programme « Critical Maritime Routes » (CMR). Il s'agit d'une série de projets axés sur le cadre juridique, les règles opérationnelles, le partage d'informations, la formation et le renforcement des capacités.
- Le Réseau interrégional du golfe de Guinée (GoGIN) vise à améliorer la connaissance du domaine maritime du réseau régional de partage d'informations de l'architecture de Yaoundé (YARIS).
- Le Soutien à la sécurité maritime intégrée en Afrique de l'Ouest (SWAIMS) vise à améliorer l'application de la loi et les cadres de gouvernance.
- Le Programme d'appui à la stratégie de sûreté et de sécurité maritimes (PASSMAR) est axé sur la coopération maritime transfrontalière.
- Le Projet de coopération portuaire (SEACOP) vise à renforcer les capacités et la coopération dans la lutte contre le trafic maritime illicite.
- Des organisations internationales telles qu'Interpol et le Programme mondial pour le démantèlement des réseaux criminels (CRIMJUST) de l'ONUDC se concentrent sur les flux du trafic de drogue.

La décision de traiter la sécurité et la cybersécurité dans les ports relève de la seule compétence du pays et l'implication d'organisations internationales doit être approuvée au niveau national.

- Le projet de sécurité portuaire en Afrique de l'Ouest et du Centre (WeCAPS),[66] un projet de la CMR dans la région du Golfe de Guinée, vise à améliorer la sécurité portuaire et à se conformer à l'ISPS. Ce projet analyse les risques dans 10 ports de la région du Golfe de Guinée et organisent des événements autour de la sécurité : formation du personnel, rencontre avec des experts et mise en œuvre du SeMS.
- L'OMI[67] et les garde-côtes américains (USCG)[68] jouent un rôle important dans les ports maritimes soumis à l'ISPS. Ils participent à plusieurs activités de formation, organisent des visites pour favoriser l'amélioration des ports et mettent en œuvre des projets d'assistance dans les ports africains.

7.4 Les cyber-risques en Afrique

Avec la numérisation croissante de l'industrie maritime et l'augmentation de la puissance des outils à la disposition des cybercriminels, le nombre de cyberattaques a augmenté, y compris les attaques contre les navires et les ports maritimes. Bien que la plupart des incidents de cybersécurité maritime n'aient pas visé les ports africains à ce jour, les preuves disponibles

[66] (WeCAPS, n.d.)
[67] (Our Work, n.d.)
[68] (Atlantic Area Units, n.d.)

de cyberattaques dans d'autres secteurs et ports fournissent des informations précieuses pour les gouvernements et les autorités portuaires africains.

Ces cyberattaques constitueraient une menace existentielle pour l'économie du continent africain si les ports étaient visés. Un récent rapport de l'Institute for Security Studies[69] sur la cybersécurité africaine dans le domaine maritime montre que la cybersécurité devient un aspect de plus en plus important eu égard des besoins de l'Afrique en matière de sécurité maritime en raison de la place grandissante que prend la numérisation dans l'industrie maritime africaine. Compte tenu de l'évolution technologique actuelle des navires, les ports africains devront renforcer leur bouclier de cybersécurité pour rester compétitifs. Il est nécessaire qu'ils réfléchissent différemment aux menaces, aux risques et aux vulnérabilités, ainsi qu'aux actes criminels.

Les navires ouvrent la voie en termes de mesures de cybersécurité et sont tenus d'inclure ces mesures dans leur manuel ISM. L'OMI et leurs compagnies d'assurance les incitent à prendre la cybersécurité au sérieux. Contrairement aux initiatives à bord des navires, les ports maritimes d'Afrique subsaharienne doivent encore relever des défis en matière de sûreté et de cybersécurité pour améliorer leur bouclier.

Une cyberattaque de grande ampleur a eu lieu en juillet 2021 sur Transnet. Cette grande société portuaire sud-africaine, qui gère 60 % du trafic de conteneurs du pays dans le port de Durban (Afrique du Sud), a été victime d'une attaque par ransomware. Cette attaque a eu pour conséquence d'engendrer des perturbations massives dans son sillage. Les terminaux à conteneurs de Durban, Ngqura, Port Elizabeth et Cape Town ont dû passer au traitement manuel des marchandises jusqu'à ce que les systèmes informatiques soient rétablis. Les camions chargés de récupérer et de décharger des conteneurs ont été bloqués pendant plus de 14 heures, et l'opérateur du terminal a inévitablement subi une perte de revenus. Dans le même rapport, ISS prédit que les incidents tels que l'attaque sur Transnet se multiplieront en Afrique subsaharienne, car les ports maritimes sont des cibles attrayantes, toujours vulnérables aux cyberattaques. Dans ce cas, les infrastructures de transport, en particulier les ports, constituent des cibles lucratives pour les cybercriminels ou d'autres acteurs hostiles en raison de l'ampleur des opérations et de l'impact médiatique international.

Bien que les principaux ports d'Afrique subsaharienne disposent de départements informatiques, la mise en œuvre et le respect de mesures concrètes de cybersécurité sont loin d'être acquis, et cette situation pose un risque évident pour la sécurité. Les décideurs politiques chargés des questions portuaires ont conscience que des progrès doivent être engrangés et manifestent un grand intérêt quant à l'amélioration du bouclier de cybersécurité pour leurs opérations et leurs systèmes de sécurité, notamment les systèmes de vidéosurveillance, de badges et de contrôle d'accès. Mais ces mêmes autorités portuaires n'ont pas suffisamment de connaissances pour améliorer leur cyber-résilience et il semble qu'il y ait peu de campagnes de sensibilisation menées par les décideurs politiques nationaux

[69] (Reva, 2020)

à l'intention des ports pour réduire les cyber-risques. Les départements de sécurité portuaire observent très peu les cyber-protocoles.[70]

L'un des projets européens dans le Golfe de Guinée (WeCAPS) a pris l'initiative de veiller à ce que le personnel portuaire à différents niveaux soit conscient des cybermenaces et des risques associés, mais également en mesure d'agir en conséquence. Il se concentre sur la formation des opérateurs et du personnel et aurait pu mener davantage d'initiatives d'amélioration au niveau des infrastructures (systèmes d'accès, de badges, de vidéosurveillance et de communication) si le temps imparti au projet l'avait permis. Le soutien apporté par ce projet est cohérent avec les meilleures pratiques mises en évidence par d'autres initiatives, notamment la publication des lignes directrices de l'IAPH 2021 sur la cybersécurité dans les ports et les installations portuaires, et les directives de l'OMI sur la gestion des risques informatiques dans le secteur maritime.

Outre l'approche ascendante de WeCAPS, une loi nationale sur la cyber-résilience serait saluée par les décideurs politiques chargés des questions portuaires. L'Union africaine a pris un départ positif en 2014 avec l'adoption de la Convention sur la cybersécurité et la protection des données personnelles (la Convention de Malabo)[71], qui pourrait être la première étape vers cette législation. En outre, les pays africains et les exploitants de terminaux privés pourraient adopter conjointement les meilleures pratiques pour assurer la sécurité de leurs infrastructures maritimes.

[70] (Africa's Maritime Cyber Security Progress After the Transnet Attack, 2021)
[71] (African Union Convention on Cyber Security and Personal Data Protection, 2014)

8 Conclusions

L'IIC maritime comprend, entre autres, les ports, les navires et les compagnies maritimes. Les IIC maritimes sont considérées comme sûres si leurs installations physiques sont sécurisées et leurs installations informatiques cybersécurisés. Cette étude a couvert tous les aspects importants pour la sécurité des IIC maritimes, notamment les aspects juridiques, politiques et technologiques, les normes et les lignes directrices.

9 Recommandations

L'objectif de cette étude n'est pas de créer un manuel de bonnes pratiques, mais de dresser une liste succincte des questions à traiter pour mettre en place un cyber-bouclier performant. Les meilleures pratiques mentionnées ci-dessous aideront les exploitants de ports et de navires à se conformer aux exigences de l'OMI en matière de gestion des risques liés à la cybersécurité, ce qui renforcera la sécurité et la fiabilité des chaînes d'approvisionnement et du commerce international.

9.1 Recommandations aux ports d'Afrique subsaharienne

Comme l'a démontré ce rapport, il est essentiel d'adopter une approche holistique de la sécurité. Ces premières recommandations portent sur la sécurité physique et complètent les recommandations énumérées plus loin visant à améliorer la cybersécurité. Les recommandations formulées dans le présent rapport se fondent sur des observations faites dans plusieurs ports d'Afrique subsaharienne, où il est possible d'améliorer le bouclier de sécurité :

1. Apporter un soutien international aux pays africains afin d'optimiser leur législation nationale en matière de sécurité maritime applicable aux zones portuaires administratives. Pour ce faire, il convient d'évaluer les règlements actuels de la police portuaire et des douanes, le code ISPS transposé dans la législation nationale, les règlements en matière de sécurité portuaire, ainsi que d'autres règlements nationaux.
2. Renforcer les capacités du personnel de sécurité par le biais de diverses initiatives, telles que :
    - La formation des pilotes de drones (contre les potentielles attaques aériennes)
    - La formation des agents de sécurité des installations portuaires au code ISPS et la formation des agents de sécurité en coopération avec l'OMI
    - Agents de sécurité avec chiens renifleurs dressés (contre les stupéfiants, les produits chimiques, les explosifs)
    - La formation du personnel de sécurité aux systèmes de gestion de la sécurité (SeMS)
    - Les conseils d'experts sur l'installation de systèmes de contrôle d'accès, de contrôle du périmètre et de centres de contrôle de la sécurité portuaire
    - La formation des équipages des embarcations pneumatiques et la formation à l'interception dans les zones portuaires
    - La formation à la surveillance pour les équipages de bateaux afin de prévenir les attaques de piraterie sur les navires au mouillage
    - La formation de la police portuaire aux tâches de sécurité portuaire et au code ISPS
    - Des formations à l'inspection et à l'audit pour les autorités compétentes et celles chargées du contrôle par l'État du port
    - La mise en place de comités de sécurité portuaire impliquant des acteurs privés et publics
3. Fournir des équipements essentiels au personnel de sécurité dans les ports et aux opérateurs privés de terminaux, afin de leur permettre de s'acquitter efficacement de leurs tâches, à savoir :

- Des drones pour la police et le personnel de sécurité
- Des bateaux pneumatiques rigides (RIB) pour les patrouilles maritimes, les agents de sécurité et la police
- De l'équipement de communication pour le personnel de sécurité sur terre et en mer
- De l'équipement d'inspection pour les agents de sécurité aux entrées des ports
- Des systèmes de balisage pour les patrouilleurs mobiles
- Des scanners à rayons X pour les douanes afin d'inspecter le fret

4. Accompagner la marine, la police, les autorités portuaires et maritimes compétentes dans leurs efforts pour améliorer les procédures opérationnelles permanentes et les plans d'intervention d'urgence dans les zones portuaires, afin de renforcer la sécurité des navires amarrés, des chenaux d'accès au port et des bassins portuaires.
5. Renforcer les relations entre les différents acteurs portuaires dans les différents pays par le biais de séminaires de partage d'expertise et d'ateliers techniques. Convier les acteurs suivants à ces événements : les ministères chargés des transports et de la sécurité nationale, les autorités compétentes, les décideurs politiques chargés des questions portuaires, les ports d'Europe et d'ailleurs, l'OMI, la Garde côtière des États-Unis, la Commission européenne, le Shipowners' Club - Protection and Indemnity (P&I) et d'autres organismes d'assurance, les compagnies maritimes et les exploitants de terminaux privés actifs sur le continent.

9.2 Recommandations aux acteurs maritimes africains

De manière générale, il est nécessaire pour les pays africains d'améliorer leur législation en matière de cybersécurité, comme beaucoup d'autres pays du monde ayant une façade maritime. Outre les initiatives en matière de sécurité portuaire, on observe que plusieurs ports doivent encore relever des défis pour rendre leur infrastructure hautement résistante aux attaques contre la sécurité et aux cyberattaques. C'est pourquoi des initiatives supplémentaires en matière de sécurité portuaire sont nécessaires pour soutenir les législateurs nationaux, les autorités portuaires, les exploitants de terminaux privés, les autorités nationales compétentes, la police, les entreprises privées de sécurité portuaire et les autres parties prenantes dans les ports et à proximité. Il est vivement recommandé de renforcer ces initiatives ISPS ainsi que les initiatives en matière de cybersécurité dans la zone portuaire juridique et administrative (sur terre et en mer). Ces initiatives permettraient de créer un cadre opérationnel, et ce de plusieurs façons : par le renforcement des capacités, le soutien au développement d'infrastructures et d'équipements appropriés, la formation et l'accompagnement, et le développement de partenariats internationaux.

9.3 Soutien de la direction générale

La direction générale est de plus en plus consciente des menaces et des risques informatiques, ainsi que de leur impact potentiellement dévastateur sur les opérations des navires et des ports. L'investissement continu nécessaire dans la cybersécurité visera spécifiquement le personnel, la gestion de la sécurité, les processus et les technologies dans ce domaine. Cette démarche nécessite l'allocation d'un budget, de ressources et doit être approuvée puis soutenue par la direction générale. Les cyber-risques peuvent à la fois toucher et être atténués par toute personne se trouvant dans les ports et à bord des navires. C'est pourquoi

les mesures en matière de cybersécurité ne doivent pas relever de la seule responsabilité du département informatique.

9.4 Sensibilisation à la cybersécurité

Toute personne à bord d'un navire ou dans un port doit être consciente des menaces et de la manière dont les incidents informatiques affectent ces infrastructures. Ces personnes doivent donc recevoir une formation de sensibilisation à la cybersécurité afin de savoir ce qu'elles peuvent faire pour garantir la sécurité d'un port et d'un navire. La formation doit être adaptée au poste.

9.5 Procédures, lignes directrices et instructions en matière de cybersécurité

Le personnel des ports et des navires doit savoir exactement ce que l'on attend de lui et comment gérer la cybersécurité. Il doit recevoir des procédures opérationnelles permanentes (POP) sur la manière de traiter les tâches quotidiennes ainsi que sur la gestion des incidents. Des équipes de cybersécurité doivent être constituées, se réunir régulièrement et avoir un impact sur les opérations.

9.6 Services et fonctions critiques de l'organisation

Pour savoir comment aborder la cybersécurité, il est essentiel de connaître les systèmes existant dans un port donné et à bord des navires. L'inventaire doit porter sur toutes les installations physiques et informatiques critiques, y compris les appareils, les systèmes, les logiciels et les applications, tant pour les TI que les TO.

9.7 Évaluation des risques liés à la cybersécurité

Une fois l'inventaire en main, il convient de procéder à une évaluation des risques afin d'identifier les menaces, les risques et les vulnérabilités liés aux installations TI et TO susceptibles d'avoir un impact négatif sur les opérations et la sécurité.

9.8 Plan de gestion de la cybersécurité

En plus des plans de sûreté (de l'installation) portuaire et des plans de sûreté des navires ISPS existants, un plan de gestion de la cybersécurité devrait être élaboré, car ces derniers sont principalement axés sur la sécurité physique. Ce genre de plan fera apparaître des mesures pour faire face aux risques identifiés sur la base d'une évaluation de risques, des responsabilités de l'équipe en matière de cybersécurité, des procédures pour répondre aux cybermenaces et des procédures d'audit des activités de cybersécurité. Ce plan comprendra des mesures procédurales et techniques à mettre en œuvre pour minimiser les cyber-risques.

9.9 Cybersécurité de la chaîne d'approvisionnement

Les fournisseurs d'équipements peuvent avoir accès à distance à des systèmes critiques à bord (systèmes de navigation, d'alimentation des moteurs, de cargaison, etc.) ou dans les installations portuaires (répartiteurs de conteneurs, grues portuaires, systèmes de grue RMG et RTG, etc.) Tout incident de cybersécurité du côté des fournisseurs peut affecter le navire ou les équipements et systèmes de manutention spécifiques dont ils sont responsables. Il est donc important d'évaluer la cybersécurité des fournisseurs afin d'identifier les risques liés à leurs services et systèmes qui pourraient avoir une incidence négative sur le fonctionnement des navires et des ports.

9.10 Gestion des incidents, réponse et rétablissement

Les navires et les ports doivent mettre en œuvre des politiques, des procédures et des contrôles appropriés qui leur permettent de détecter les incidents de cybersécurité, d'y répondre, de se rétablir et d'en tirer des enseignements.

9.11 Normes et cadres en matière de cybersécurité

Il n'est pas facile de gérer tous les aspects de la gestion de la cybersécurité sans recourir à l'aide et aux conseils des normes et lignes directrices existantes. Par conséquent, la gestion de la cybersécurité devrait s'appuyer sur des politiques, des processus et des procédures concernant les contrôles techniques et la sensibilisation du personnel pour gérer la cybersécurité dans les ports et à bord des navires. Pour éviter les erreurs, il est important de s'appuyer sur les conseils d'experts maritimes, qui peuvent aider à mettre en œuvre la cybersécurité dans l'environnement des ports et des navires.

9.12 Recommandations générales pour les ports en matière de cybersécurité

Les recommandations en matière de cybersécurité énumérées ci-dessous et à mettre en œuvre dans les ports maritimes pourraient avoir un impact positif sur la cybersécurité des autorités portuaires et des autres parties prenantes exerçant une activité dans le port.

1. Législation en matière de cybersécurité dans les ports

La mise en œuvre/mise en conformité du droit national avec la législation, les lignes directrices et les codes internationaux en matière de cybersécurité portuaire est la clef d'un commerce international qui inspire confiance.

2. Évaluation de la cybersécurité (CSA)

Conformément aux normes de sécurité ISPS, des évaluations de la sécurité (PSA et PFSA) sont effectuées pour les ports et les installations portuaires. L'objectif de ces évaluations est d'identifier les vulnérabilités des structures physiques, des systèmes de protection du personnel et des processus opérationnels qui pourraient conduire à un incident de sécurité. L'évaluation de la cybersécurité doit s'appuyer, le cas échéant, sur les évaluations existantes de la sécurité en vertu du code ISPS. Il convient d'avoir recours aux normes actuelles (ISO270xx) et aux meilleures pratiques internationales (IMO/BIMCO, ENISA, IACS) pour évaluer, estimer et atténuer les risques informatiques et physiques.

3. Plan de cybersécurité (CSP)

Les évaluations de la sécurité constituent la base des plans de sûreté des ports (PSP) et des installations portuaires (PFSP). Ces plans prennent en compte les questions identifiées dans l'évaluation correspondante en établissant des mesures de sécurité appropriées conçues pour minimiser la probabilité d'une violation de la sécurité et les conséquences des risques potentiels. Le plan de cybersécurité doit s'appuyer sur le PSP ou le PFSP existant si nécessaire. Il est également important de tester le plan, de préférence au moyen d'exercices de mise en situation, afin de s'assurer qu'il est à jour et compris par toutes les parties prenantes.

Un CSP a la même fonction que le plan de sécurité ISPS pour les questions identifiées dans l'évaluation de la cybersécurité. Il tient également compte de l'impact des mesures énoncées dans le PSP et le PFSP.

4. Organisation informatique

Pour la gestion de la cybersécurité, il est essentiel de disposer d'un organigramme dans lequel les différentes parties prenantes se voient attribuer des rôles et des tâches spécifiques.

- La nomination d'un agent chargé de la cybersécurité des navires (SCSO). Ce dernier serait responsable de la cybersécurité du port et des infrastructures portuaires gérées par le port.
- La mise en place d'un comité de sécurité portuaire auquel participent différentes parties prenantes.
- La mise en place d'un centre d'opérations de sécurité (COS).

5. Gestion de la cybersécurité

Une fois le bouclier de cybersécurité installé suite à la mise en œuvre du processus d'évaluation de la cybersécurité et du CSP, il est important que le COS soit géré de manière appropriée et dispose de mécanismes opérationnels, notamment :

- Audit et examen réguliers du CSP
- Tests réguliers de cyberattaque
- Suivi de l'évolution du bouclier de cybersécurité
- Méthodes pour fournir des informations à des tiers
- Comment gérer les incidents de sécurité
- Tests réguliers des plans et de la gestion d'incident par le biais d'exercices de mise en situation.

6. Formation au renforcement des capacités

Le personnel travaille avec des systèmes TO et TI. Par conséquent, il est nécessaire qu'il bénéficie d'une formation régulière pour travailler efficacement. C'est pourquoi la formation à différents niveaux est essentielle :

- Formation du personnel de sécurité (opérateurs) qui utilise quotidiennement les systèmes de sécurité TO et TI.
- Formation à la gestion de la sécurité (PFSO, PSO) afin de saisir les conséquences et l'impact sur la sécurité des systèmes TI et TO. Le personnel doit être en mesure de minimiser les dommages, de mettre en œuvre des contre-mesures de sécurité immédiates et de revenir à une situation opérationnelle normale le plus rapidement possible.
- Formation du personnel informatique qui travaille avec des systèmes de sécurité TO. Ces personnes doivent être en mesure d'installer et d'améliorer le bouclier de cybersécurité pour le personnel de sécurité.

Les recommandations de sécurité ci-dessus sont présentées dans le tableau suivant :

N°	Recommandations
1	Optimiser les législations nationales en matière de sécurité maritime (règlements de la police portuaire et des douanes, règlements nationaux ISPS et de sécurité portuaire)
2	Formation des agents de sécurité des installations portuaires au code ISPS et formation des agents de sécurité avec le concours de l'OMI

3	Agents de sécurité avec chiens / formation aux barrières intelligentes (contre les stupéfiants, les produits chimiques, etc.)
4	Formation du personnel de sécurité aux systèmes de gestion de la sécurité (SeMS)
5	Conseils sur l'installation de systèmes de contrôle d'accès, de contrôle du périmètre et la mise en place de centres de contrôle de la sécurité portuaire
6	Formation des équipages d'embarcations pneumatiques et formation à l'interception dans les zones portuaires
7	Formation à la surveillance pour les équipages de bateaux afin de prévenir les attaques de piraterie sur les navires au mouillage
8	Formation de la police portuaire aux tâches de sûreté portuaire et au code ISPS
9	Formations à l'inspection et à l'audit pour les autorités compétentes et celles chargées du contrôle par l'État du port
10	Mise en place de comités de sécurité portuaire impliquant des acteurs privés et publics
11	Fournir des équipements de sécurité certifiés pour le personnel de sécurité dans les ports et pour les opérateurs de terminaux privés (drones, RIBS, équipements de communication, équipements d'inspection, systèmes de balisage et scanners à rayons X).
12	Accompagner le procureur, la police et la marine pour améliorer les procédures opérationnelles permanentes et les plans d'intervention d'urgence (sur terre et en mer).
13	Renforcer les relations entre les différents acteurs portuaires dans le monde.
14	Améliorer la législation, les pratiques et les procédures nationales en matière de cybersécurité dans les ports
15	Évaluation et gestion de la cybersécurité
16	Établir, mettre en œuvre, auditer et améliorer en permanence le plan de cybersécurité
17	Nommer un responsable de la cybersécurité et une équipe de cybersécurité
18	Mettre en place un comité de sécurité portuaire
19	Mettre sur pied et gérer un COS
20	Organiser un groupe de gestion quotidienne pour traiter les incidents et les autres tâches quotidiennes liées à la cybersécurité.
21	Formation du personnel de sécurité (opérateurs de sécurité)
22	Formation à la gestion de la sécurité (PFSO, PSO)
23	Formation du personnel informatique qui travaille avec des systèmes de sécurité TO.

9.13 Recommandations à l'UE : vers une collaboration stable entre l'UE et l'Afrique

Une collaboration entre l'UE et l'Afrique dans les domaines suivants renforcerait la sécurité maritime mondiale et la sécurité de nos chaînes d'approvisionnement :

- *Développer des collaborations stables* entre les ministères chargés de la mer et des transports, les agences de sécurité et les ISACs maritimes afin de parvenir à une compréhension commune, à une surveillance continue, à l'atténuation des problèmes

de sécurité et des incidents de sécurité transfrontaliers dans l'écosystème maritime. Créer des synergies fortes et échanger des connaissances, des recommandations et des bonnes pratiques.

- *Campagnes de sensibilisation et formation à la sûreté maritime* : Établir une collaboration avec des entités publiques et privées pour développer des centres de sensibilisation à la sécurité maritime, mais également organiser des entraînements opérationnels et des formations au traitement des incidents qui ciblerait les besoins généraux en matière de sécurité maritime et de sécurité spécifique au transport maritime. Ces formations seraient accompagnées de plateformes de simulation et d'exercice qui faciliteraient le développement des compétences.
- *Combler le fossé en matière de compétences informatiques* grâce à des évaluations pratiques des risques, à la simulation virtuelle d'attaques et d'incidents industriels ciblant le secteur du transport maritime et l'écosystème numérique de la chaîne d'approvisionnement maritime et internationale. L'utilisation intensive des plateformes de simulation cyber peut aider les acteurs du secteur du transport maritime à mieux comprendre la gestion d'attaques et d'incidents complexes, et à améliorer la préparation et la résilience du secteur du transport maritime. L'idée serait de mener des expériences en conditions réelles fondées sur des cas concrets et des exercices de « capture du drapeau » avec des équipes de cybersécurité et d'attaque s'affrontant les unes contre les autres. L'Association internationale des sociétés de classification (AISC) et l'OMI peuvent s'appuyer sur l'expérience d'ENISA-Cyber Europe et continuer à collaborer avec l'ENISA et la CERT-UE pour promouvoir la formation à la cybersécurité et ouvrir la voie à une formation efficace dans le secteur maritime.
- *Soutien transfrontalier à l'exploitation de COS maritimes* permettant de prévoir et de gérer efficacement les cyberattaques et les incidents de sécurité.
- *Harmoniser les efforts de certification maritime* : Auditer et évaluer conjointement la sécurité des équipements maritimes afin de garantir le respect de la confidentialité, la sécurité, la transparence, l'interopérabilité, la responsabilité et la conformité avec la législation et les lignes directrices de l'UE et de la communauté internationale en matière de sécurité. Encourager les communautés européennes et africaines (militaires et civiles) de fabricants, de développeurs et d'intégrateurs à adopter une culture de partage des responsabilités en matière de sécurité en effectuant des tests de conformité communs à l'aide de normes internationales.
- *Évaluer* régulièrement en procédant à des analyses comparatives entre les ports de l'UE, d'Afrique subsaharienne et d'autres régions du monde, telles que l'Asie du Sud-Est. Il serait alors possible de mettre en évidence les approches fructueuses de l'UE et de l'Afrique en matière de sécurité et de cybersécurité. Ces dernières pourraient ainsi être émulées dans d'autres régions.

10 Références bibliographiques

(s.d.). Récupéré sur https://issafrica.s3.amazonaws.com/site/images/2021-02-10-gulf-of-guenea-piracy-map.png

Acharya, T. (2019, July 31). *Black boxes and their intrusion*. Récupéré sur Towards Data Science: https://towardsdatascience.com/black-boxes-and-their-intrusion-620aa3c4c56b

Africa Maritime Technology Cooperation Centre launched in Mombasa. (2017, December 13). Récupéré sur EEAS: https://www.eeas.europa.eu/node/37286_en

(2014). *African Union Convention on Cyber Security and Personal Data Protection.* African Union. Récupéré sur https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Africa's Maritime Cyber Security Progress After the Transnet Attack. (2021, September 16). Récupéré sur The Maritime Executive: https://maritime-executive.com/article/africa-s-maritime-cyber-security-progress-after-transnet-attack

Alcaide, J. I., & Garcia-Llave, R. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia, 45*, 547-554. doi:10.1016/j.trpro.2020.03.058

Alderton, P. (1999). *Port Management and Operations.* LLP Professional Publishing. Récupéré sur https://commons.wmu.se/cgi/viewcontent.cgi?article=1070&context=all_dissertations

Ashraf, I., Park, Y., Hur, S., Kim, S., Alroobaea, R., Bin Zikria, Y., & Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1-14. doi:10.1109/TITS.2022.3164678

Atlantic Area Units. (s.d.). Récupéré sur United States Coast Guard Atlantic Area: https://www.atlanticarea.uscg.mil/Our-Organization/Area-Units/

Burt, J. (2021, August 10). Cybersecurity Landscape and Threats to Maritime Operations. Récupéré sur https://www.tenntom.org/wp-content/uploads/2021/10/CISA-Jason-Burt_CISA_Cybersecurity-Port_Maritime-Security.pdf

China hackers steal data from US Navy contractor - reports. (2018, June 9). Récupéré sur BBC: https://www.bbc.com/news/world-us-canada-44421785

Code of Safe Practice for Cargo Stowage and Securing (CSS Code). (s.d.). Récupéré sur IMO: https://www.imo.org/en/OurWork/Safety/Pages/CSS-Code.aspx

Company, R. (2017, July 21). *How ports can protect themselves against cyber and physical security threats*. Récupéré sur Medium: https://medium.com/@ICHCA/how-ports-can-protect-themselves-against-cyber-and-physical-security-threats-b6bd10c4f7a7

Costa Concordia: What happened. (2015, February 10). Récupéré sur BBC: https://www.bbc.co.uk/news/world-europe-16563562

Coulibaly, S., Kassa, W., & Zeufack, A. (2022, June). *Re-engineering African trade with the European Union and United States: Success requires reform on both sides*. Récupéré sur World Bank Blogs: https://blogs.worldbank.org/africacan/re-engineering-african-trade-european-union-and-united-states-success-requires-reform

Darbra, R.-M., & Casal, J. (2004, February). Historical analysis of accidents in seaports. *Safety Science, 42*(2), 85-98. doi:10.1016/S0925-7535(03)00002-X

Directive (UE) 2016/1148 du Parlement Européen et du Conseil 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 (2016). Récupéré sur https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148

Drougkas, D. A., Sarri, A., Kyranoudi, P., & Zisi, A. (2019, November 26). *Port Cybersecurity - Good practices for cybersecurity in the maritime sector.* ENISA. Récupéré sur ENISA: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

(2022). *ENISA Threat Landscape 2022.* European Union Agency for Cybersecurity (ENISA). Récupéré sur https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Erstad, E., Ostnes, R., & Lund, M. (2021, March). An Operational Approach to Maritime Cyber Resilience. *TransNav, 15*(1). doi:10.12716/1001.15.01.01

ESPO: The First Port of Call for European Transport Policy Makers in Brussels. (s.d.). Récupéré sur ESPO: https://www.espo.be/

EU-Africa: Global Gateway Investment Package. (s.d.). Récupéré sur European Commission: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en

European Maritime Safety Agency . (s.d.). Récupéré sur EMSA: https://www.emsa.europa.eu/

European Union Agency for Cybersecurity (ENISA). (2020). ENISA Threat Landscape: 15 Top Threats in 2020. Récupéré sur https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape-2020-top-15-threats

(2020). *Good Practice Guide: Cyber Security for Ports and Port Systems.* The Institution of Engineering and Technology. Récupéré sur https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

Greater and More Diverse Participation in Global Trade is Key to Achieving Africa's Economic Transformation, says New World Bank Book. (2022, February 10). Récupéré sur The World Bank: https://www.worldbank.org/en/news/press-release/2022/02/10/greater-and-more-diverse-participation-in-global-trade-is-key-to-achieving-africa-s-economic-transformation-says-new-wor

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Récupéré sur Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(2020). *Guidelines - Cyber Risk Management for Ports.* European Union Agency for Cybersecurity (ENISA). Récupéré sur https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

(2017). *Guidelines on Maritime Cyber Risk Management.* London: IMO. Récupéré sur https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

Gulf of Guinea Map. (2021). Récupéré sur https://issafrica.s3.amazonaws.com/site/images/2021-02-10-gulf-of-guenea-piracy-map.png

Hand, M. (2020, April 17). *MSC confirms malware attack caused website outage*. Récupéré sur Seatrade Maritime News: https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

Herald of Free Enterprise Ferry Disaster – 1987. (s.d.). Récupéré sur Devastating Disasters: https://devastatingdisasters.com/herald-of-free-enterprise-ferry-disaster-1987/

ILO: International Labour Oeganization. (s.d.). Récupéré sur UN: Office of the Secretary-General's Envoy on Youth: https://www.un.org/youthenvoy/2013/08/ilo-international-labour-organization/?gclid=CjwKCAiAv9ucBhBXEiwA6N8nYF5eTI5UjefYhsbZBgjQa8jYr3hWW0MocPuYj4mAk-nPawYFcgjb1hoCS3QQAvD_BwE

International Convention for the Safety of Life at Sea (SOLAS), 1974. (s.d.). Récupéré sur IMO: https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 197. (s.d.). Récupéré sur IMO: https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Convention.aspx

Inventory of Risk Management / Risk Assessment Methods and Tools . (s.d.). Récupéré sur European Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory

ISO/IEC 27001 and related standards: Information security management. (s.d.). Récupéré sur ISO: https://www.iso.org/isoiec-27001-information-security.html

Jørgensen, R. N. (2018). *Cyber security survey shows more action is needed in the industry*. Récupéré sur BiMCO: https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

Kalogeri, E., & Polemi, N. (2022). A taxonomy of maritime security standards. *6th NMIOTC Conference on Cyber Security in Maritime Domain.* Souda Bay: NATO.

Kioskli, K., & Polemi, N. (2020). A Socio-Technical Approach to Cyber-Risk Assessment. *International Journal of Electrical and Computer Engineering, 14*(10), 305-309. Récupéré sur https://publications.waset.org/10011507/a-socio-technical-approach-to-cyber-risk-assessment

Kioskli, K., & Polemi, N. (2020). Psychosocial Approach to Cyber Threat Intelligence. *International Journal of Chaotic Computing, 7*(1), 159-165. doi:10.20533/ijcc.2046.3359.2020.0021

Langewiesche, W. (2004, May). A Sea Story. *The Atlantic.* Récupéré sur https://www.theatlantic.com/magazine/archive/2004/05/a-sea-story/302940/

Maritime trade and Africa. (2018, October 3). Récupéré sur UNCTAD: https://unctad.org/press-material/maritime-trade-and-africa

(2021). *Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities.* IMO. Récupéré sur https://events.iala-aism.org/content/uploads/2021/09/MSC-104-7-1-IAPH-Cybersecurity-Guidelines-for-Ports-and-Port-Facilities-IAPH.pdf

Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø., & Nesheim, D. (2021, September). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, 15*(3). doi:10.12716/1001.15.03.04

MTCC Africa. (s.d.). Récupéré sur MTCC Africa: http://mtccafrica.jkuat.ac.ke/

Negreiro, M. (2022). *The NIS2 Diretive: A high common level of cybersecurity in the EU.* Récupéré sur https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

NIST Risk Management Framework (RMF). (s.d.). Récupéré sur NIST: Computer Security Resource Center: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/

Our Work. (s.d.). Récupéré sur IMO: https://www.imo.org/en/OurWork/Pages/Default.aspx

Polemi, N. (2017). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains.* Elsevier. doi:9780128118191

Port of San Diego: phishing emails remain amongst greatest cyber threats. (2021, August 19). Récupéré sur Port Technology International: https://www.porttechnology.org/news/port-of-san-diego-phishing-emails-remain-amongst-greatest-cyber-threats/#:~:text=The%20Port%20of%20San%20Diego%20reported%20a%20ransomware,hacker%20operating%20inside%20the%20Islamic%20Republic%20of%20Iran.

Resolution A.682 (17). (1991). International Maritime Organization. Récupéré sur https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.682(17).pdf

Reva, D. (2020). *Maritime cyber security: Getting Africa ready.* Institute for Security Studies. Récupéré sur https://issafrica.s3.amazonaws.com/site/uploads/ar-29-2.pdf

(s.d.). *Rulebook 2021.* UKP&I. Récupéré sur https://www.ukpandi.com/news-and-resources/rulebook-2021/

Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports. (s.d.). Récupéré sur CORDIS: https://cordis.europa.eu/project/id/740477

Shapira, I. (2006, January 4). Captain Blamed in Fatal Tanker Explosion Off Va. *The Washington Post*. Récupéré sur https://www.washingtonpost.com/archive/local/2006/01/04/captain-blamed-in-fatal-tanker-explosion-off-va/f4a4ffc8-6cea-4893-ba6c-e9afd76eec8d/

SOLAS XI-2 and the ISPS Code. (s.d.). Récupéré sur IMO: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Standards. (s.d.). Récupéré sur ISO: https://www.iso.org/standards.html

(2018). *Strenghtening Africa's gateways to trade.* PwC. Récupéré sur https://www.pwc.co.za/en/assets/pdf/strengthening-africas-gateways-to-trade.pdf

The Beirut Port Explosion. (s.d.). Récupéré sur Forensic Architecture: https://forensic-architecture.org/investigation/beirut-port-explosion

(2020). *The Guidelines on Cyber Security onboard Ships - Version 4.* BIMCO. Récupéré sur https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

The International Safety Management (ISM) Code. (s.d.). IMO. Récupéré sur https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx

(2021). *Threat Landscape for Supply Chain Attacks.* European Union Agency for Cybersecurity (ENISA). Récupéré sur https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Titanic. (s.d.). Récupéré sur Britannica: https://www.britannica.com/topic/Titanic/Aftermath-and-investigation#ref302525

Tomter, L., & Gundersen, M. (2019, April 14). *IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre*. Récupéré sur NRK: https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043

WeCAPS. (s.d.). Récupéré sur Strengthening the security and safety of ports in West and Central Africa : https://wecaps.eu/en/

Widup, S. (2019). *2019 Verizon Data Breach Investigations Report.* Verizon. Récupéré sur https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf

Winder, D. (2019, July). *U.S. Coast Guard Issues Alert After Ship Heading Into Port Of New York Hit By Cyberattack*. Récupéré sur Forbes: https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=78d82cb141aa

11 Annexes : Questionnaires portant sur la sécurité

11.1 Annexe A : Questionnaire sur la sensibilisation à la gouvernance de la sécurité

Basé sur la norme ISO27001[72], le questionnaire suivant peut servir à évaluer la structure de gouvernance d'une entreprise maritime afin de gérer les risques de sécurité :

Objectif de contrôle	Sujet	Question	Non	Oui
Politique de sécurité (sûreté et cybersécurité)	Politique de sécurité de l'information	Le personnel connaît-il la politique de sécurité liée à ses fonctions ?		
Organisation de la sécurité	Organisation interne	Le personnel est-il conscient de ses responsabilités en matière de sécurité ?		
		Le personnel dispose-t-il des autorisations nécessaires ?		
	Acteurs extérieurs	Le personnel est-il conscient des risques possibles lorsqu'il traite avec des acteurs extérieurs ?		
		Le personnel prend-il des mesures de sécurité lorsqu'il traite avec les clients ?		
Gestion des installations	Responsabilité des installations	Le personnel connaît-il les installations auxquelles il a affaire ?		
		Le personnel connaît-il le propriétaire de ces installations ?		
		Le personnel sait-il à quoi servent ces installations ?		
	Classification des informations	Le personnel connaît-il les lignes directrices en matière de classification ?		
		Le personnel connaît-il les informations relatives à l'étiquetage et à la manipulation ?		
Sécurité des ressources humaines	Pendant la période d'emploi	Le personnel connaît-il ses responsabilités en matière de gestion ?		
		Le personnel a-t-il reçu une formation de sensibilisation à la sécurité dans les domaines de la sûreté (par ex., les mesures de contrôle d'accès) et de la cybersécurité (par ex., hameçonnage, ingénierie sociale, stockage de données) ?		

[72] A partir de l'Organisation internationale de normalisation (ISO) ; https://www.iso.org/isoiec-27001-information-security.html

	Fin d'emploi	Le personnel sait-il qu'en cas de cessation du contrat de travail, il doit restituer son équipement et que les droits d'accès lui sont retirés ?		
Sécurité physique et environnementale	Zones sécurisées	Le personnel connaît-il le périmètre de sécurité physique du port ?		
		Le personnel est-il au courant des contrôles d'entrée physique ?		
		Le personnel connaît-il la procédure de sécurisation du lieu de travail ?		
	Sécurité des équipements	Le personnel sait-il comment utiliser les équipements de sécurité et les équipements informatiques dans les locaux ?		
		Le personnel est-il au courant de la politique relative à l'utilisation des appareils personnels sur le lieu de travail ?		
		Le personnel connaît-il les procédures relatives à l'élimination ou à la réutilisation en toute sécurité des équipements ?		
Gestion des communications et des opérations	Procédures opérationnelles et responsabilités	Le personnel connaît-il les procédures opérationnelles liées aux activités ?		
		Le personnel est-il au courant du processus de gestion des modifications ?		
	Protection contre les codes malveillants et les codes d'applications mobiles	Le personnel est-il au courant des contrôles contre les codes malveillants (par ex., traitement des courriels) ?		
		Le personnel est-il au courant des contrôles contre les codes d'applications mobiles (c'est-à-dire les appareils mobiles infectés) ?		
	Sauvegarde	Le personnel est-il au courant du processus de sauvegarde des informations ?		
	Traitement des supports	Le personnel est-il sensibilisé à la gestion des supports amovibles ?		
		Le personnel est-il au courant des modalités d'élimination des supports ?		

		Le personnel connaît-il les procédures de traitement de l'information ?		
		Le personnel est-il sensibilisé à la sécurité de la documentation du système ?		
	Échange d'informations	Le personnel est-il sensibilisé à la protection des supports physiques en transit ?		
		Le personnel est-il au courant de l'existence de la messagerie électronique ?		
	Services maritimes électroniques	Le personnel connaît-il la procédure relative aux transactions en ligne et à l'utilisation d'informations accessibles au public ?		
	Contrôle	Le personnel est-il au courant de la politique concernant les registres ?		
Contrôle d'accès	Exigences de la société en matière de contrôle d'accès	Le personnel connaît-il la politique de contrôle d'accès ?		
	Gestion de l'accès des utilisateurs	Le personnel connaît-il la procédure d'enregistrement des utilisateurs ?		
		Le personnel est-il au courant de la politique/gestion des mots de passe des utilisateurs ?		
		Le personnel connaît-il la procédure relative aux droits d'accès des utilisateurs ?		
	Responsabilités de l'utilisateur	Le personnel est-il sensibilisé à l'utilisation de mots de passe ?		
		Le personnel est-il au courant de la procédure à suivre en cas d'utilisation non supervisée de l'équipement ?		
		Le personnel est-il au courant de la politique relative au retrait de tout matériel sensible de l'espace de travail si ce dernier est laissé sans surveillance par son utilisateur ?		
	Contrôle d'accès au réseau	Le personnel connaît-il la politique d'utilisation des services de réseau ?		
	Contrôle d'accès au système d'exploitation	Le personnel connaît-il les procédures de connexion sécurisée ?		
		Le personnel sait-il comment utiliser des utilitaires système ?		

	Contrôle d'accès aux applications et aux informations	Le personnel connaît-il les restrictions d'accès à l'information ?		
		Le personnel est-il sensibilisé à la protection de l'isolement des systèmes sensibles ?		
	Informatique mobile et travail à distance	Le personnel connaît-il la politique appliquée en matière d'informatique et communication mobiles ?		
		Le personnel connaît-il la politique relative à l'utilisation des technologies portuaires/navales et des systèmes de travail à distance ?		
Acquisition, développement et maintenance des systèmes d'information	Contrôles cryptographiques	Le personnel connaît-il la politique d'utilisation des clés cryptographiques et du matériel connexe ?		
Gestion des incidents liés à la sécurité de l'information	Signaler les événements et les failles en matière de sécurité de l'information	Le personnel connaît-il les procédures de signalement des événements liés à la sécurité de l'information ?		
		Le personnel connaît-il les procédures de signalement des failles de sécurité ?		
Gestion de la continuité des activités	Gestion de la continuité des activités	Les employés connaissent-ils le plan de continuité des activités et le plan de reprise après sinistre liés à leurs fonctions ?		

11.2 Annexe B : Questionnaire sur les pratiques de sécurité

Le questionnaire suivant peut être distribué aux ports afin d'évaluer la maturité de leurs pratiques en matière de cybersécurité. Il peut également être distribué aux compagnies maritimes et aux armateurs pour qu'ils établissent un rapport et évaluent les pratiques de sécurité mises en œuvre et suivies :

Questionnaire sur la sensibilisation à la sécurité destiné aux opérateurs portuaires et maritimes

Informations (facultatif)

Entreprise	xxxxxx
Nom	xxxxx
Position	xxxxx
Nombre de salariés	xxxxx
Activité de l'entreprise	xxxx
Site internet	xxxxx
Adresse mail	xxxxxx

Date

A toutes les parties prenantes maritimes,

L'objectif de ce questionnaire est de comprendre le niveau de sensibilisation à la sécurité de l'infrastructure maritime critique (IC) en termes de menaces et de vulnérabilité de toutes les couches de l'IC, c'est-à-dire (a) l'infrastructure physique, (b) l'équipement de l'infrastructure télécom (c) les logiciels (d) les services et les applications (e) les données (f) les utilisateurs (personnes et objets externes/internes). En outre, nous cherchons à obtenir une vue d'ensemble des services et des utilisateurs à travers le prisme de la vulnérabilité.
Le questionnaire vise à déterminer si :

- Les opérateurs maritimes ont mis en place un plan de sûreté (plan de sûreté portuaire et politique de sécurité des TIC) dont ils connaissent le degré d'application et les objectifs ;
- Les employés et les utilisateurs maritimes sont conscients des problèmes de sécurité liés à leurs activités quotidiennes ;
- La formation de sensibilisation à la sécurité de l'information est proposée et son efficacité évaluée ;
- Les relations entre les autorités compétentes et l'IC maritime (par ex., les ports) existent et pour quelles raisons.

Dans le cadre de cette enquête, seuls les IC maritimes en tant qu'opérateurs sont pris en compte (c'est-à-dire les ports qui sont à la fois propriétaires et opérateurs OU opérateurs de terminaux). Bien que l'enquête porte sur les ports, elle s'applique à toutes les IC maritimes.

Les réponses sont confidentielles et seuls des chiffres globaux seront communiqués.

Pour plus d'informations, vous pouvez contacter :

xxxxxx

Plan de sûreté portuaire

1. Le port dispose-t-il d'un plan de gestion de la sécurité bien défini ?

☐ Oui ? Passez aux question 1a
☐ Non ? Passez à la question 2

1a. Quel modèle de gestion de la sécurité adoptez-vous ? [Ne choisir qu'une seule réponse]

☐	Interne. C'est-à-dire, par un département spécifique ou un (des) employé(s) du port (par ex., le(s) PFSO)
☐	Externe. C'est-à-dire, par une autre entreprise, une organisation ou un (des) expert(s) externe(s)
☐	Autre

1b. Quelle proposition décrit le mieux votre perception de la sécurité : [Choisissez-en une seule]

☐	Ne concerne pas / n'influence pas vos activités commerciales
☐	Ce n'est pas votre première priorité, mais vous envisagez de la prendre en compte à l'avenir
☐	Vous comprenez sa nécessité, mais son coût est trop élevé pour l'envisager

1c. Quels sont les normes de sécurité couvertes par votre plan de sécurité ? [Choisissez autant de réponses que nécessaires]

☐	ISPS
☐	ISO 9001, ISO 14001 (Services des ports de croisière)
☐	ISO 27001
☐	ISO 27002
☐	ISO 28000
☐	Autre : PERS (Système d'évaluation environnementale du port, pour l'ensemble de la zone portuaire)
☐	Autre (laquelle :_____)

1d. Votre plan de sécurité identifie-t-il et analyse-t-il en profondeur les éléments suivants ?

Activités	Notre plan de sécurité ne couvre pas cet élément.	Notre plan de sécurité couvre cet élément, et...	
		les parties prenantes présentent des documents valables, mais nous ne les analysons pas.	nous gardons une base de données active et disposons de processus spécifiques et détaillés pour les analyser
Plans de sûreté des navires	☐	☐	☐
Agents de sûreté des navires	☐	☐	☐
Agents de sûreté de la compagnie	☐	☐	☐
Équipement à bord	☐	☐	☐
Plans de sécurité des infrastructures portuaires correspondantes	☐	☐	☐
Agents de sécurité de l'installation portuaire	☐	☐	☐
Certains équipements de sécurité	☐	☐	☐
Certains dispositifs de sécurité	☐	☐	☐
Contrôle des activités des personnes et des marchandises	☐	☐	☐
Communications sécurisées	☐	☐	☐
Accès sécurisé dans les secteurs portuaires (surveillance, contrôle)	☐	☐	☐
Politique « Cyber Port »	☐	☐	☐
Autre (à préciser)	☐	☐	☐
Je ne sais pas	☐		

2. Avez-vous pris en compte les questions de sécurité dans les activités suivantes du port au cours des 12 derniers mois ? Si oui, vos réactions ont-elles été proactives ou réactives ?

Activités	Les questions de sécurité n'ont pas été prises en compte	Oui, les questions de sécurité ont été prises en compte	
		Nature de l'action	
		proactive	réactive
Amélioration de vos services/produits/activités/chaînes d'approvisionnement	☐	☐	☐
Conformité du secteur	☐	☐	☐
Amélioration du fonctionnement de vos systèmes informatiques	☐	☐	☐
Amélioration du fonctionnement des systèmes d'entrée/sortie/de contrôle du périmètre de vos installations portuaires	☐	☐	☐
Amélioration de l'image de votre entreprise, du niveau de confiance de vos utilisateurs et de vos services	☐	☐	☐
L'alignement avec la législation européenne influence vos opérations internationales et vos chaînes d'approvisionnement	☐	☐	☐
Confidentialité et protection des données	☐	☐	☐
Sécurité du personnel et des utilisateurs	☐	☐	☐
Accès sécurisé dans les secteurs portuaires	☐	☐	☐
Je ne sais pas	☐		

3. Sélectionnez trois (3) grandes catégories de réglementations/législations qui ont influencé/influenceront votre fonctionnement et vos mesures de sécurité au cours des 12 derniers mois/prochains mois. Indiquez si vous envisagez de mettre en place des projets de sécurité.

Types de règlements	Au cours des 12 derniers mois	Au cours des 12 prochains mois	Projets de sécurité en cours/envisagés
Audit interne :			
ISPS	☐	☐	☐
ISM	☐	☐	☐
Familles de normes ISO	☐	☐	☐
Familles OHSAS 18000	☐	☐	☐
Sarbanes-Oxley	☐	☐	☐
Règlement (CE) 725/2004	☐	☐	☐
Normes SOLAS/MARPLE			
Directive 2008/114/CE du Conseil concernant le recensement et le classement des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.	☐	☐	☐
Protection des données (par ex., RGPD, NIS, NISII, ISO 27000/27001/27002/27005, ISO15048, ISO18045)	☐	☐	☐
Réglementations sectorielles (par ex., norme de sécurité des données PCI)	☐	☐	☐
Règlements des douanes et des autorités financières	☐	☐	☐
Autre (problèmes avec les douanes _____)	☐	☐	☐
Autre (aucun problème avec les autorités financières _____)	☐	☐	☐
Autre (précisez_____)	☐	☐	☐

4. Sélectionnez cinq (5) problèmes de cybersécurité en termes d'importance (1 = la plus faible, 5 = la plus élevée) pour votre société. Disposez-vous d'un plan pour résoudre ces problèmes ?

Problèmes liés à la cybersécurité	Problème de sécurité important	Plan de réponse		
		Maintenant	au cours des 12 prochains mois	Pas de plan
Diffusion sécurisée des données (aux autorités compétentes, aux fournisseurs de la chaîne d'approvisionnement, aux compagnies maritimes, etc.)	☐	☐	☐	☐
Stockage sécurisé des données	☐	☐	☐	☐
Accès (physique) aux installations portuaires (entrée/sortie)	☐	☐	☐	☐
Services portuaires sécurisés (gestion des conteneurs, GNL, services de la chaîne d'approvisionnement)	☐	☐	☐	☐
Identificateurs par radiofréquences (RFID)	☐	☐	☐	☐
Appareils mobiles (par ex., assistant numérique personnel, smartphones)	☐	☐	☐	☐
Procédure automatisée de contrôle aux frontières (ABC)	☐	☐	☐	☐
Stockage mobile (par ex., clé USB, disques durs portables)	☐	☐	☐	☐
Téléphonie IP	☐	☐	☐	☐
Services Web	☐	☐	☐	☐
Réseaux Wi-Fi	☐	☐	☐	☐
Communication sécurisée par satellite	☐	☐	☐	☐
Nouveaux systèmes d'exploitation	☐	☐	☐	☐
Cryptographie des courriers électroniques	☐	☐	☐	☐
Cryptographie de disque dur	☐	☐	☐	☐

Pratiques de sécurité

5. Comment vérifiez-vous le niveau de sécurité de votre entreprise ?

[Choisissez plus d'une réponse si nécessaire]

- ☐ Audit interne (effectué par le département chargé de la sécurité)
- ☐ Audit externe
- ☐ Évaluation interne réalisée par le personnel

☐ Autre
☐ Nous ne disposons pas de telles procédures

6. Sélectionnez cinq (5) activités principales de sécurité en termes d'importance (1 = la plus faible, 5 = la plus élevée) pour votre port. Sélectionner de manière indépendante cinq (5) activités principales de sécurité en fonction du temps de mise en œuvre nécessaire (1 = mise en œuvre rapide, 5 = chronophage) :

	Importance	**Temps de mise en œuvre**
Conformité avec le code ISPS	☐	☐
Conformité avec les normes ISO27001 et 27005	☐	☐
Gestion de la continuité des activités	☐	☐
Gestion des risques et de la sécurité	☐	☐
Poursuite, développement et intégration des systèmes informatiques	☐	☐
Gestion de l'accès et du contrôle	☐	☐
Communication et gestion des opérations	☐	☐
Sécurité physique	☐	☐
Protection des employés (sûreté)	☐	☐
Mises à jour des services et des produits	☐	☐
Gestion de la sécurité	☐	☐
Politique de (cyber) sécurité	☐	☐
Confidentialité - Protection des données	☐	☐
Responsabilité	☐	☐
Plan de reprise après sinistre	☐	☐

7. Comment abordez-vous / résolvez-vous les problèmes de sécurité suivants dans votre port :

Problèmes de sécurité :	Nous n'en tenons pas compte	Meilleures pratiques	Nos propres méthodes
Incidents de cybersécurité - Attaques	☐	☐	☐

Problèmes de sécurité :	Nous n'en tenons pas compte	Meilleures pratiques	Nos propres méthodes
Continuité des activités	☐	☐	☐
Résilience de la société	☐	☐	☐
Gestion des risques informatiques	☐	☐	☐
Gestion des risques physiques	☐	☐	☐
Confidentialité et protection des données	☐	☐	☐
Mécanismes de sécurité dans les services portuaires proposés	☐	☐	☐

8. Lorsque vous collaborez avec d'autres entreprises (par ex., sous-traitants, entrepreneurs externes, tiers), quels sont les éléments suivants que vous considérez comme nécessaires en matière de sécurité ?

- ☐ Vos collaborateurs disposent d'une politique de sécurité vérifiable et la respectent.
- ☐ Vos collaborateurs sont tenus d'utiliser votre propre politique de sécurité et de respecter vos préoccupations en matière de sécurité.
- ☐ Vos collaborateurs sont conformes à la norme ISO 27001
- ☐ Aucune de ces réponses
- ☐ Autre

9. Avez-vous déjà procédé à une évaluation des risques physiques ?

- ☐ Oui
- ☐ Non

10. À quelle fréquence et à qui signalez-vous les risques et les incidents liés à la sécurité physique ?

	Fréquence				
	Tous les jours	Tous les mois	Tous les 3 mois	Tous les 6 mois	Jamais
Agent de sûreté des installations portuaires	☐	☐	☐	☐	☐
Entreprise de sécurité (externe)	☐	☐	☐	☐	☐

	Fréquence				
	Tous les jours	Tous les mois	Tous les 3 mois	Tous les 6 mois	Jamais
Police	☐	☐	☐	☐	☐
Douanes	☐	☐	☐	☐	☐
Autorités compétentes (lesquelles : _____)	☐	☐	☐	☐	☐
Compagnies d'assurance	☐	☐	☐	☐	☐
Banques et institutions financières	☐	☐	☐	☐	☐
Entrepreneurs et parties prenantes	☐	☐	☐	☐	☐
Chambre de commerce (ou organisation similaire)	☐	☐	☐	☐	☐
Autorité nationale de certification	☐	☐	☐	☐	☐
Autre (spécifiez_____)	☐	☐	☐	☐	☐
Autre (spécifiez_____)	☐	☐	☐	☐	☐
Autre (spécifiez_____)	☐	☐	☐	☐	☐

11. Avez-vous déjà procédé à une évaluation des risques informatiques ?

☐ Oui
☐ Non

12. À quelle fréquence et à qui signalez-vous les risques et les incidents liés à la cybersécurité ?

	Fréquence				
	Tous les jours	Tous les mois	Tous les 3 mois	Tous les 6 mois	Jamais
Agent chargé de la cybersécurité du port	☐	☐	☐	☐	☐
Entreprise de sécurité (externe)	☐	☐	☐	☐	☐
Autorités publiques (par ex., police)	☐	☐	☐	☐	☐
Compagnie maritime	☐	☐	☐	☐	☐
Autorités compétentes (par ex., CERT, CSIRTS, ISAC, ministère)	☐	☐	☐	☐	☐

	Fréquence				
	Tous les jours	Tous les mois	Tous les 3 mois	Tous les 6 mois	Jamais
Compagnies d'assurance	☐	☐	☐	☐	☐
Banques et institutions financières	☐	☐	☐	☐	☐
Entrepreneurs et parties prenantes	☐	☐	☐	☐	☐
OMI, AESM (ou organisation maritime similaire)	☐	☐	☐	☐	☐
Autorité nationale de certification	☐	☐	☐	☐	☐
Autre (spécifiez_____)	☐	☐	☐	☐	☐
Autre (spécifiez_____)	☐	☐	☐	☐	☐
Autre (spécifiez_____)	☐	☐	☐	☐	☐

13. Comment vous informez-vous sur les questions de sécurité ? Quelle organisation serait la plus appropriée pour donner une formation sur la sécurité ? Quels sont les sujets qui vous intéressent le plus ? (Vous pouvez faire plusieurs choix)

Organisations	Technologies et mise en œuvre de la sécurité	Politiques de sécurité	Évaluation des risques	Protection de la confidentialité et des données
Consultants en sécurité (entreprises privées)	☐	☐	☐	☐
Université	☐	☐	☐	☐
Organe national	☐	☐	☐	☐
Internet	☐	☐	☐	☐
Organisme gouvernemental	☐	☐	☐	☐
Chambres de commerce	☐	☐	☐	☐
Associations industrielles ou organismes professionnels (par ex., OMI,	☐	☐	☐	☐

Organisations	Technologies et mise en œuvre de la sécurité	Politiques de sécurité	Évaluation des risques	Protection de la confidentialité et des données
AESM, ENISA, NIST)				
Presse, publications scientifiques	☐	☐	☐	☐

14. Quelles sont les normes de sécurité que vous connaissez ?

- ISO 9001 ☐
- ISPS ☐
- ISM ☐
- Inspections SIRE / ATB ☐
- ISA/IEC-62443 ☐
- Inspection de barges et de bateaux de navigation intérieure (États-Unis) ☐
- Inspection EBIS ☐
- ISO/IEC 2700x ☐
- ISO 20858 ☐
- ISO 15408, ISO18045 ☐
- Forum sur la sécurité de l'information ☐
- CobIT ☐
- ITIL (ensemble d'ouvrages recensant les bonnes pratiques de la gestion d'un système d'information) ☐
- CMMI (modèle d'évaluation du niveau de maturité d'une structure concernant le développement de systèmes, de produit ou de logiciels) ☐
- SEISMED ☐
- Aucune de ces réponses ☐
- Autre (précisez_____) ☐
- Autre (précisez_____) ☐

Ajoutez si nécessaire

15. Quel est le statut de votre port en ce qui concerne les activités de sécurité suivantes :

Activité	En place/ En cours	En place dans les 12 prochains mois	Non prévue
Accès physique à l'aide de cartes à puce	☐	☐	☐
Accès physique à l'aide de cartes d'identification sur papier	☐	☐	☐
Accès physique à l'aide de procédures automatisées de contrôle aux frontières (ABC)	☐	☐	☐
Utilisation de différentes technologies d'authentification pour l'accès physique (par ex., cartes de proximité, cartes à puce, biométrie)	☐	☐	☐
Utilisation de systèmes de détection d'intrusion	☐	☐	☐
Filtres anti-virus et anti-spam récents	☐	☐	☐
Utilisation de pare-feu	☐	☐	☐
Inspections (hors calendrier) sur les navires	☐	☐	☐