Garde côtière canadienne | Canadian Coast Guard

LA JOURNÉE DE L'INDUSTRIE : CYBERSÉCURITÉ MARITIME DU NAVIRE À LA CÔTE

RAPPORT SUR LES RÉSULTATS ET LA VOIE À SUIVRE

Canada

La journée de l'industrie : Cybersécurité maritime du navire à la côte - Rapport sur les résultats et la voie à suivre

Publié avec l'autorisation de la :

Pêches et Océans Canada
Garde côtière canadienne
Ottawa (Ontario) K1A 0E6

Fs23-707/2023F-PDF
978-0-660-48381-8

2023-04-18

Disponible sur le site intranet de la GCC

Available in English:
Industry Day : Maritime cybersecurity from ship-to-shore - Results and path forward Report

Cat. No. Fs23-707/2023E-PDF
ISBN: 978-0-660-48380-1

Table des matières

Résumé

La Garde côtière canadienne (Garde côtière) a organisé une « Journée de l'industrie sur la cybersécurité maritime : du navire à la côte », durant laquelle se sont réunies des parties prenantes de l'industrie, du gouvernement et du milieu universitaire pour discuter des cyberrisques maritimes et évaluer les options permettant d'assurer la cyberrésilience du secteur maritime. Cette activité d'une journée entière, qui s'est tenue le 2 février 2022, a connu une forte affluence, ayant accueilli près de 300 participants virtuels venus s'informer sur les dernières menaces à la cybersécurité dans le secteur maritime.

Durant la journée, des représentants de ministères fédéraux, de chargeurs canadiens, d'autorités portuaires, d'entreprises de cybersécurité maritime et de sociétés de classification des navires, des premiers intervenants maritimes nationaux et internationaux, des experts en cybersécurité et des organismes de réglementation ont fait des présentations. Ces échanges entre diverses parties prenantes du secteur maritime ont permis de mieux faire connaître les auteurs des menaces et l'incidence de celles-ci, et d'échanger quant aux meilleures façons d'assurer la résilience de ce secteur essentiel, malgré un niveau inédit de connectivité entre les systèmes de technologie de l'information (TI) et de technologie opérationnelle (TO).

Les principaux sujets abordés ont été les suivants : comment accroître la cyberrésilience du secteur maritime (p. ex. la cybersécurité des navires, des ports et des terminaux de marchandises), la nécessité d'une formation accrue sur la cybersécurité maritime, le financement des ports de taille moyenne à petite, la création et le maintien en poste d'une main-d'œuvre solide en matière de cybersécurité et l'augmentation de la mise en commun d'information sur les cyberrisques.

Le présent rapport sur les résultats et la voie à suivre contient des recommandations en vue d'une collaboration pour la formation sectorielle sur la cybersécurité maritime, du financement de la cybersécurité maritime et de la mise en commun d'information sur la cybersécurité, ainsi que concernant les chaînes d'approvisionnement en matière de cybersécurité maritime et les autorités chargées de la cybersécurité maritime.

Présentation

Comme le Canada est une nation maritime, l'industrie maritime s'est avérée essentielle à son développement. L'industrie maritime a influé sur le développement économique national, l'emplacement et la croissance des villes, ainsi que sur les moyens de subsistance des Canadiens depuis des générations. L'industrie du transport maritime contribue au PIB du Canada à hauteur de trois milliards de dollars par an et fait partie du secteur des infrastructures de transport essentielles. Indirectement, l'industrie maritime contribue à l'emploi de plus de 100 000 Canadiens et génère 4,6 milliards de dollars en revenu du travail[1]. Le commerce maritime permet la mise en place de chaînes d'approvisionnement mondiales et régionales qui soutiennent le fonctionnement de la vie quotidienne des Canadiens.

En 2017, consciente de l'augmentation exponentielle des cyberattaques dans le secteur maritime, l'Organisation maritime internationale (OMI), institution spécialisée relevant des Nations Unies, a publié une résolution qui oblige les navires de classe « sauvegarde de la vie humaine en mer » (SOLAS, ou *Safety of Life at Sea*) à mettre en œuvre des mesures pour contrer les cyberrisques dans les systèmes de gestion de la sécurité de leur organisme au plus tard le 1er janvier 2021. Les cyberattaques maritimes ont eu des répercussions non seulement sur les navires et leur fonctionnement, mais aussi sur les ports et les exploitants de terminaux, ce qui s'est répercuté sur les opérations et a causé des centaines de millions de dollars en dommages en raison de pertes de données et de retards dans la livraison de marchandises.

Selon une entreprise de cybersécurité maritime, le montant moyen versé aux cybercriminels pour une attaque dans le secteur maritime est estimé à 3,1 millions de dollars américains[2]. En outre, les acteurs étatiques et leurs intermédiaires ciblent activement les systèmes de navigation, de communication et de contrôle industriel des navires, des ports et des terminaux portuaires afin d'infliger un maximum de dommages.

Les systèmes non sécurisés et non segmentés peuvent rendre l'équipement maritime inopérant et entraîner une série de répercussions importantes dans ce secteur essentiel. En soi, la Garde côtière n'est pas à l'abri des tentatives d'auteurs malveillants d'attaquer les systèmes essentiels, y compris les systèmes de communications maritimes. Si ces systèmes étaient interrompus lors d'une intervention de recherche et de sauvetage, il se pourrait que les messages de détresse ne soient pas reçus. Par conséquent, il est essentiel que le

gouvernement continue d'établir des approches communes pour la mise en commun de l'information sur la cybersécurité maritime avec les nations alliées et l'industrie.

Or, l'atténuation des cyberrisques exige non seulement de comprendre la convergence entre les systèmes de TI et de TO, mais aussi de savoir comment ces systèmes varient par rapport aux TI génériques. Par exemple, bien que les employés qui occupent des postes à bord de navires ou à terre disposeront d'une messagerie électronique et d'une connexion Wi-Fi, tout comme les employés de bureau, ce qui rend le secteur unique, ce sont les systèmes de navigation (systèmes de cartographie électronique, de visualisation et d'information, GNSS, radar), les systèmes de contrôle industriel (SCI) (par exemple manutention de cargaison, interface homme-machine, propulsion/direction, TO), les systèmes de communication (SIA, liaison satellite, voix sur IP), ainsi que les systèmes de chargement et de stabilité (par exemple, les systèmes de coque/ballast, de filtration de l'eau). De même, les emplois à terre dans les ports doivent composer avec un problème parallèle, soit celui de la complexité de leurs systèmes, des commandes de portiques, des systèmes SCADA, des automates programmables, ainsi que des communications et des serveurs informatiques qui sont hors site. De la même manière, le transport maritime de marchandises dépend de nombreux SCI et systèmes de TI, par exemple des centres de données des chargeurs, d'infrastructures de TI ou de systèmes de TO, lesquels influent sur les systèmes de surveillance des citernes qui assurent la sécurité du transport et du stockage du pétrole et du gaz naturel. En raison du croisement entre les exigences essentielles en matière de sécurité et les capacités de surveillance à distance, la surveillance de ces systèmes entraîne un potentiel de cyberincident, à moins qu'ils ne soient correctement sécurisés et segmentés.

La variété et la complexité de ces systèmes, et la vitesse à laquelle ils se connectent à Internet, n'ont pas suivi le rythme des mesures de sécurité destinées à les protéger des auteurs malveillants. La Garde côtière joue un rôle de premier plan en tant qu'acteur dans ce segment des infrastructures essentielles, et ce de nombreuses façons : prévention des inondations par le déglaçage ou le dégagement des voies de navigation de la glace pour assurer la prospérité économique; lutte contre la pollution; intervention d'urgence ainsi que recherche et sauvetage; soutien à l'application de la loi; et assurance de la souveraineté du Canada dans les eaux arctiques. Outre les services qu'elle assure depuis longtemps, la Garde côtière utilise une approche tous risques pour veiller à ce que l'intervention fondée sur les risques dans le contexte de la cybersécurité maritime soit proactive et non réactive.

L’état de la cybersécurité maritime

Au cours des vingt dernières années, le contexte de la sécurité a connu un changement d’orientation, passant d’activités centrées sur la sécurité physique à une gestion des cybermenaces résultant de l’interconnectivité croissante. Les gouvernements et l’industrie n’ont pas été en mesure de suivre le rythme de l’interconnectivité entre les TI et les TO dans leurs interventions. En 2019, une enquête a révélé que 68 % des fabricants comptent augmenter leurs investissements dans la convergence TI-TO au cours des deux prochaines années. En 2020, plus de 500 cyberattaques graves de systèmes de TO ont été dénombrées dans le secteur maritime. Ces données sont significatives, car les ports et les navires dépendent d’une combinaison de systèmes de TI et de TO, ce qui témoigne d’une vulnérabilité accrue aux cybermenaces dans le secteur maritime.

Si des gains en efficacité peuvent aider le secteur à atteindre ses objectifs financiers, les logiciels non sécurisés ou l’équipement maritime non segmenté peuvent avoir des effets en cascade si le cyberrisque n’est pas dûment pris en charge. Depuis le début de la pandémie, en 2020, une entreprise de cybersécurité a noté une augmentation de 400 % des tentatives de piratage des systèmes informatiques et de TO de l’industrie maritime, et une hausse de 900 % des cyberattaques visant les TO des ports et des navires[3]. Pendant six jours, en 2021, le canal de Suez s’est retrouvé bloqué par le mégaconteneur *Ever Given.* Cet événement a engendré des pertes de 400 millions de dollars américains par heure, soit une perte commerciale totale estimée de 54 milliards américains pour l’économie mondiale. Si cet incident était le fruit de simples vents violents, une cyberattaque pourrait certainement entraîner l’échouement ou le chavirement d’un navire. Ces exemples montrent à quel point la menace du cyberrisque maritime est réelle pour la sécurité et la prospérité économique des navires dans les eaux canadiennes.

Dans les terminaux portuaires, les cyberattaques sur les systèmes de contrôle d’accès peuvent avoir des effets extrêmement perturbateurs. Par exemple, la plupart des grues des ports intelligents sont construites et exploitées par une seule entreprise à l’étranger et fonctionnent sur des réseaux 5G et avec d’autres services automatisés. Si cette entreprise était touchée par une cyberattaque ou contrainte par une entité publique d’arrêter le fonctionnement de ces grues, cela entraînerait un arrêt effectif de ses activités et bloquerait par ricochet les activités de ports dans tout le Canada en quelques secondes à peine[4]. En 2019, un cabinet de recherche a mis au jour une opération semblable en prenant le contrôle de plusieurs grandes grues.

Selon des sources ouvertes, il existe de bonnes raisons de croire que certains acteurs étatiques hostiles ciblent à distance les systèmes de contrôle industriel et les systèmes de contrôle et d'acquisition de données (SCADA) des navires, par exemple les systèmes relatifs à l'eau de ballast et à la filtration, dans l'intention de couler les navires et de causer des dommages irréparables ainsi que des pertes humaines. Certains États-nations détiennent une base de données des vulnérabilités de l'équipement maritime dans le but d'exploiter de telles fragilités au maximum en temps de guerre ou si des sanctions accrues leur seraient imposées[5,6]. Cela se produit dans un contexte où les États hostiles s'affairent à accroître leurs cybercapacités offensives.

Les chaînes d'approvisionnement en cybersécurité maritime sont également les cibles privilégiées de cyberattaques. En 2019, des menaces persistantes avancées (MPA) parrainées par l'État ont ciblé des universités au Canada dans le but d'acquérir des technologies maritimes et navales. Or, de tels renseignements ont une valeur très élevée pour les nations adverses. Grâce à eux, elles peuvent exercer une influence sur une marine ou une garde côtière étrangère et sur ses priorités intellectuelles. Une fois qu'ils ont accédé aux chaînes d'approvisionnement, les auteurs de menaces peuvent chercher à perturber les activités essentielles des navires ainsi que les services de communication maritime essentiels.

Les États hostiles cherchent activement à exploiter l'équipement de communication maritime à la recherche de dispositifs exposés à Internet qui sont utilisés à l'échelle mondiale afin d'accéder aux écrans de connexion des recherches sur Internet. Ces acteurs mettent à profit des sites Web comme *Shodan* pour montrer comment les appareils et les systèmes d'information sont connectés à Internet et comment ils peuvent être surveillés et contrôlés à distance. Cela soulève la question des dispositifs connectés à Internet, de l'intégrité de l'équipement maritime et des fabricants d'équipement d'origine (FEO) pour garantir la confidentialité, l'intégrité et l'accessibilité ainsi que la qualité des matériaux utilisés pour fabriquer cet équipement.

Il existe de nombreux exemples où des cyberattaques visant des systèmes de TI ont eu des répercussions sur les TO. Par exemple, en 2019, la United States Coast Guard (garde côtière américaine) est intervenue sur un navire désemparé et infecté dont les systèmes n'étaient pas sécurisés et non segmentés. Un rançongiciel se serait introduit dans le système de TO du navire, rendant le navire inopérant.

Selon certains spécialistes du secteur qui ont étudié l'industrie maritime en 2021, parmi les cyberattaques perpétrées, 40 % étaient des attaques importantes ou graves, tandis que 52 % étaient des incidents mineurs. En ce qui concerne la formation à la cybersécurité, seuls 26 % des sondés estiment que les efforts de sensibilisation à la cybersécurité sont suffisants. En outre, seule la moitié des personnes interrogées ont déclaré s'être vu proposer une forme de formation à la cybersécurité. En ce qui concerne les systèmes de TI et de TO, l'inclusion d'une formation à la cyberhygiène contribuerait à atténuer les risques pour l'humain dans le secteur maritime.

Une nouvelle étude de recherche menée par une société de cybersécurité maritime en 2022 a révélé que, dans les cas de cyberattaques dans le secteur maritime qui ont donné lieu au paiement d'une rançon, les armateurs ont versé en moyenne plus de 3,1 millions de dollars américains aux cybercriminels. Cette étude a en outre révélé que les armateurs sous-investissent considérablement dans la gestion de la cybersécurité, la majorité d'entre eux consacrant moins de 100 000 dollars américains par an à la cybersécurité. Ce manque d'investissement pourrait s'expliquer par le fait que les entreprises se laissent bercer par un faux sentiment de sécurité, conséquence de la sous-déclaration endémique du nombre réel de cyberattaques.

De nombreux organismes maritimes n'ont pas encore pris conscience du risque pour les systèmes et de l'éventail des menaces auquel ce secteur est confronté. En 2017, l'OMI a adopté la résolution MSC.428(98) *Gestion des cyberrisques maritimes dans les systèmes de gestion de la sécurité* (Maritime Cyber Risk Management in Safety Management Systems), une résolution exigeant que les armateurs et exploitants de navires mettent en œuvre des considérations de cybersécurité dans leurs systèmes de gestion de la sécurité au plus tard le 1er janvier 2021. Bien que de telles résolutions internationales soient importantes et qu'elles aient conduit de nombreuses associations internationales à établir des lignes directrices et des exigences, certains critiquent un manque de structure de gouvernance, qui empêcherait de faire progresser d'autres questions, par exemple celle de l'interconnexion.

La Garde côtière est un propriétaire et un exploitant d'infrastructures essentielles qui est responsable de ses actifs et de ses services, qu'il s'agisse du déglaçage des voies de navigation pour le commerce, du déglaçage pour prévenir les inondations, du soutien à l'application de la loi, des interventions d'urgence, de la recherche et du sauvetage, de l'assurance de la souveraineté dans les eaux canadiennes, de l'intervention en cas de pollution, des services de trafic maritime et de communication ainsi que des aides à la navigation. Il est

de la responsabilité première des propriétaires et des exploitants d'infrastructures essentielles de renforcer la résilience de ces infrastructures pour faire face aux perturbations et aux catastrophes prévisibles. En raison des niveaux exponentiels de connectivité et de la convergence des systèmes de TI et de TO, le secteur maritime doit collectivement se préparer à l'inévitable.

Par son rôle de coprésident du partenariat CAN-US MDA : *Cyber assessment working group* (Groupe de travail sur la cyberévaluation), la Garde côtière continue d'attirer l'attention sur l'interconnexion du secteur maritime et sur ses vulnérabilités. En outre, en dirigeant l'atelier sur la cybersécurité de l'Association Internationale de Signalisation Maritime (2021) et en présidant le groupe de travail sur la cybersécurité du partenariat MDA du Groupe des cinq (Gp5) nouvellement créé (2022), la Garde côtière continue de faire progresser ses connaissances sur la situation relative aux menaces du point de vue des marins et sur comment atténuer les pires scénarios. Il faut pour cela reconnaître que toutes les parties prenantes du secteur maritime jouent un rôle dans ce secteur d'infrastructures de transport essentielles. Ce n'est qu'en réunissant l'industrie et le gouvernement pour exposer les menaces communes et harmoniser les efforts que de véritables progrès pourront être réalisés.

Journée de l'industrie : Résumé des discussions en groupe et thématiques

Aperçu du groupe de discussion 1 : Certification et notation de classe en matière de cybersécurité maritime

Ce groupe de discussion s'est penché sur les mesures prises par certains spécialistes du secteur pour fournir à la main-d'œuvre les compétences et outils nécessaires pour comprendre le contexte des menaces de cybersécurité maritime.

Discours d'ouverture par le directeur général, Flotte et Services maritimes de la Garde côtière canadienne. Ce groupe de discussion était modéré par la Garde côtière canadienne, et comportait des experts de Bureau Veritas, Neptune Cyber et Nettitude (une société de LRQA).

Résumé

- Les frontières entre les systèmes de TI et de TO s'estompant, les scénarios les plus pessimistes deviennent de plus en plus une réalité en raison du degré d'interconnexion entre le navire et la terre.

- La formation à la cybersécurité maritime est la plus efficace des mesures que les organismes peuvent adopter. Or, cette responsabilité ne concerne pas seulement les spécialistes des TI, mais aussi l'ensemble du personnel.

- Les perturbations du spectre par usurpation d'identité (*spoofing*) ou par brouillage entraînent des risques importants pour la navigation, puisque de telles attaques manipulent les systèmes d'infrastructures essentielles, par exemple les systèmes d'identification automatique (SIA).

Discussion thématique

Tous les mois, le nombre de cyberattaques bat de nouveaux records. En 2021, les attaques de cybersécurité ont coûté environ 6 billions (6 000 milliards) de dollars américains dans le monde entier. D'ici 2025, ce montant atteindra probablement 10,5 billions de dollars américains. Les États-nations et les cybercriminels mènent des opérations et surveillent les organismes maritimes tous les jours. Les auteurs de menaces passent par ces surfaces exposées, soit par le navire, soit par l'intermédiaire de l'entreprise. S'il existe un moyen de compromettre un navire, ce même moyen pourrait servir à compromettre tous les navires de la flotte.

À mesure que les pirates informatiques élargissent leurs sphères d'attaque et trouvent de nouveaux moyens de compromettre les systèmes, les scénarios catastrophes, comme les pannes touchant une flotte tout entière, sont devenus une réalité. La frontière entre les TI et les TO est plus difficile à définir, d'où une vulnérabilité qui peut être exploitée sur des centaines de navires. Les auteurs de menaces pourraient tirer avantage d'un manque de culture numérique au sein d'un organisme et, une fois à l'intérieur des systèmes de réseau d'un navire, on ne sait pas dans quelle mesure il serait difficile pour eux de pouvoir manipuler à distance la direction, les pompes à ballast et les systèmes de navigation du navire. Le secteur maritime est confronté à des problèmes fondamentalement différents de l'environnement de bureau en matière de cybersécurité. Les navires sont désormais interconnectés d'une manière qui pose un problème à ceux qui n'ont pas reçu de formation en cybersécurité maritime. Les armateurs et exploitants de navires doivent être en mesure d'identifier les actifs de TI/TO et la manière dont ils sont interconnectés ou reliés à la terre.

Par exemple, le réseau interne d'un navire s'interconnecte avec divers systèmes nécessaires au maintien à flot du navire, ainsi qu'avec un réseau externe pour le faire fonctionner efficacement. L'*International Association of Classification Societies* (IACS) reconnaît le risque que représentent les navires non sécurisés et non segmentés. Pour y remédier, elle a adopté en 2022 deux nouvelles exigences unifiées assorties d'exigences minimales fondées sur des objectifs de cyberrésilience des nouveaux navires et de cybersécurité des systèmes et de l'équipement embarqués. Ces exigences unifiées s'appliqueront aux nouveaux navires dont la construction est prévue à compter du 1er janvier 2024[7]. Aussi, la cybersécurité devra être prise en compte tout au long du cycle de vie du navire, depuis la phase de conception jusqu'aux phases de construction, d'exploitation, de maintenance et de mise hors service. Certains grands chantiers navals s'affairent déjà à mettre en œuvre cette exigence avec l'aide des sociétés de classification et des entreprises de cybersécurité maritime.

La formation à la cybersécurité maritime est l'une des mesures les plus importantes et les plus efficaces que le secteur maritime puisse prendre. Une telle formation doit viser l'ensemble du personnel, non pas seulement les spécialistes des TI. L'OMI attend de chaque organisme qu'il prenne des mesures efficaces, par l'intermédiaire de son système de gestion de la sécurité, pour gérer les cyberrisques. Parmi les mesures d'atténuation, notons la présence à bord de membres d'équipage ayant des responsabilités particulières en matière de cybersécurité. Il pourrait s'agir d'assurer la présence à bord d'un capitaine de navire ou d'un responsable de TI chargé de mettre à jour les systèmes informatiques, d'appliquer les derniers correctifs logiciels

et de tenir à jour les cartes et autres systèmes de navigation. Pour de nombreux travailleurs qui ont un emploi à terre et qui travaillent avec des systèmes de TI génériques, cela signifie qu'ils doivent observer les principes de base de la cyberhygiène. Il est de plus en plus attendu des armateurs et exploitants de navires qu'ils se dotent d'une cyberculture. Il suffit d'un seul employé non formé pour que, sans le savoir, un rançongiciel se propage dans le système d'une entreprise, entraînant des millions de dollars de dommages ou rendant ses activités inopérantes.

L'usurpation du SIA est un autre exemple d'attaque relativement facile à mettre en œuvre pour les auteurs de menaces; or, des solutions innovantes seront nécessaires pour fournir une défense suffisante contre ces attaques. Les entreprises de cybersécurité maritime collaborent avec le milieu universitaire, par exemple l'École Polytechnique Montréal, afin de trouver des solutions innovantes pour détecter et empêcher ces types de cyberattaques de se produire.

Aperçu du groupe de discussion 2 : Orientations en matière de cybersécurité maritime et gestion des risques liés à la chaîne d'approvisionnement électronique

Ce groupe de discussion a passé en revue les lignes directrices en matière de cybersécurité maritime recommandées aux armateurs, aux exploitants et aux ports à l'échelle tant nationale qu'internationale. En outre, il s'est penché sur les différents risques liés aux chaînes d'approvisionnement en cybersécurité maritime.

Le groupe de discussion était dirigé par Bastionnage Consulting Inc. et composé d'experts de Transports Canada (TC), de la fonction publique et du secteur de l'approvisionnement du Canada, et de la Garde côtière des États-Unis.

Résumé

- Les chaînes d'approvisionnement électronique maritime sont menacées non seulement par les matériaux de contrefaçon, mais aussi par les portes dérobées des systèmes informatiques exploitées par les méthodes sophistiquées des acteurs étatiques et de leurs intermédiaires.

- La certification *Cybersecurity Maturity Model* (CMMC) renforce la confiance des consommateurs envers la capacité d'un organisme à élaborer des produits et services fondés sur l'approche de la sécurité dès le stade de la conception.

- La garde côtière américaine renforce la capacité de son cybereffectif à détecter les menaces et à se défendre contre ceux qui cherchent à perturber le secteur maritime.

Discussion thématique

Une entreprise de technologie a récemment fait l'objet d'une cyberattaque qui s'est propagée à ses clients et a échappé à toute détection pendant plusieurs mois. Les pirates avaient utilisé un logiciel malveillant qui créait une porte dérobée dans les systèmes informatiques des clients et installait un logiciel malveillant. L'incident a conduit au vol de propriété intellectuelle et d'informations sensibles. Les chaînes d'approvisionnement du secteur de la défense et du secteur maritime sont des cibles de choix pour les cyberattaques. En 2019, des événements parrainés par l'État ont ciblé les universités du Canada dans le but d'acquérir des technologies maritimes.

Le département de la Défense américain est en tête pour ce qui est de l'adoption de la cybercertification par les fournisseurs de sa chaîne d'approvisionnement. Notamment, il a adopté une nouvelle réglementation exigeant que tous les entrepreneurs de sa chaîne d'approvisionnement soient accrédités selon les normes de la CMMC. Le gouvernement du Canada évalue les options sur la façon de répondre aux exigences de cybersécurité de la chaîne d'approvisionnement dans le contexte du CMMC. De nombreux organismes, par exemple le département de la Défense américain, prennent très au sérieux la sécurité dès la conception et acquièrent de l'équipement maritime uniquement auprès de fournisseurs ayant reçu la certification CMMC.

La nécessité d'adopter une certification de la chaîne d'approvisionnement en matière de cybersécurité a été mise en avant. Cette certification favorise le consumérisme intelligent : la sécurité dès la conception tout au long du cycle de vie des ports, des navires et des terminaux portuaires. Ceci revêt une grande importance, car les portes dérobées des systèmes de TI et le manque de sensibilisation aux cyberrisques peuvent entraîner un relâchement des normes lors de l'achat de matériel électronique. Vu la nature interconnectée des systèmes de TI, de TO et de navigation maritime, les vulnérabilités des chaînes d'approvisionnement peuvent avoir des effets domino catastrophiques. Aussi, l'insécurité dans la chaîne d'approvisionnement d'un fournisseur peut se répercuter aux produits d'autres fournisseurs une fois ceux-ci intégrés au navire ou au port. Il existe des moyens de contrôle physique pour protéger les vies et les biens, par exemple des escortes par des moyens nautiques lorsqu'un navire pourrait être compromis.

En réponse aux attentats du 11 septembre, la garde côtière américaine a élaboré un cadre de cybersécurité qui exige des exploitants maritimes qu'ils évaluent leurs systèmes, leurs réseaux et leurs installations pour y déceler les vulnérabilités, et qu'ils élaborent un plan de sécurité pour combler ces lacunes. Grâce à une collaboration interorganismes, la garde côtière américaine a renforcé la résilience des réseaux dans le but d'atténuer les incidents avant qu'ils ne surviennent.

Dans le cadre de son rôle en matière de cybersécurité, la garde côtière américaine vise à devenir un chef de file reconnu dans le domaine de la sécurité et de la sûreté maritimes en établissant de solides partenariats public-privé dans le but d'ouvrir le dialogue avec les parties prenantes, améliorer la cyberconscience et renforcer les processus de mise en commun d'information. Les efforts de sensibilisation doivent couvrir les cybermenaces, les risques, les vulnérabilités et les pratiques exemplaires, et prévoir la participation à des ateliers et des conférences, ainsi que des mesures de sensibilisation du public. La garde côtière américaine

fournit des conseils à l'industrie et aux parties prenantes par l'intermédiaire des profils du cadre de cybersécurité, de la circulaire 01-20 *Navigation and Vessel Inspection Circular* (NVIC), de sa directive de travail sur la gestion des cyberrisques liés aux navires, ainsi que de son modèle d'évaluation des cyberrisques maritimes en cours d'élaboration. En outre, la garde côtière américaine a retenu les services de conseillers en sécurité maritime et en cybersécurité pour aider à former la main-d'œuvre maritime et a intégré la cyberhygiène à ses inspections maritimes générales de routine.

Aperçu du groupe de discussion 3 : Sécurité cyber-physique et systèmes de contrôle industriel

Ce groupe de discussion s'est penché sur la sécurité physique des SCI ainsi que sur les services et formations en matière de cybersécurité disponibles pour le secteur maritime. En outre, il a exploré la possibilité de collaborer à un échange accru de renseignements et à la création d'une communauté de pratique sur la cybersécurité maritime.

Le troisième groupe de discussion était dirigé par Bastionnage Consulting Inc. et réunissait des experts de l'Association des administrations portuaires canadiennes, de Canada Steamship Lines Groupe Inc., de Sécurité publique Canada (SPC) et du Centre canadien pour la cybersécurité (CCC).

Résumé

- Le gouvernement du Canada continue de faire progresser les politiques en matière de cybersécurité maritime en matière de normes, d'échange de renseignements, de coordination et de prise de décision.
- Les ports, les navires et les terminaux portuaires sont exposés à des vulnérabilités accrues en raison de leur dépendance permanente à l'égard des systèmes informatiques, de TO et de positionnement, navigation et synchronisation (PNS).
- Il faut investir davantage dans la formation afin de mieux préparer la prochaine génération de spécialistes de la cybersécurité.

Discussion thématique

Les ports, les exploitants de navires et les entreprises de cybersécurité maritime ont réclamé davantage de renseignements sur les cyberrisques, compte tenu de leur incidence sur les activités commerciales. De plus, les chargeurs canadiens et l'Association des autorités portuaires canadiennes ont indiqué qu'ils verraient un avantage supplémentaire à la tenue régulière d'une tribune pour l'échange de renseignements dans la foulée de l'activité en cours.

Le groupe de discussion a mis en évidence la nécessité d'une sensibilisation accrue à la convergence des TI et des TO et de déterminer comment les responsables d'infrastructures essentielles et les intervenants en gestion des urgences devront collaborer pour établir des processus décisionnels.

Il est souvent difficile de savoir où trouver une formation et de l'information concrètes sur les TO propres au secteur. L'investissement dans la formation en matière de cybersécurité fait actuellement défaut. Un petit nombre d'universités et de collèges, comme l'École Polytechnique de Montréal, mènent des travaux en cybersécurité maritime propre au domaine. Si plusieurs établissements d'enseignement proposent des formations en cybersécurité liées aux infrastructures essentielles, peu d'entre elles concernent directement le secteur maritime. Les chargeurs maritimes canadiens ont noté qu'il existe une corrélation directe entre les investissements réalisés dans la formation des étudiants en cybersécurité et le secteur de l'industrie où ils choisissent de travailler. Les États-Unis, le Royaume-Uni et Israël ont déjà réalisé de tels investissements dans des secteurs d'expertise précis.

Au Canada, les autorités portuaires font preuve de vigilance. Nombre d'entre elles ont élaboré leurs propres capacités d'intervention en matière de cybercriminalité. Cependant, la majorité des 550 ports de taille moyenne à petite ne disposent pas des ressources dont disposent les grands ports et manquent donc de capacité d'intervention en cybersécurité. L'AAPC souligne qu'une cyberattaque pourrait avoir un effet « boule de neige » sur la chaîne d'approvisionnement régionale des petits ports, selon le type d'incident. Il est nécessaire de disposer d'un cadre de cybersécurité approprié dans ce secteur et de se doter d'une capacité d'intervenir efficacement en cas de pertes de vies humaines, de pollution ou d'obstacles aux voies de navigation (par exemple, un navire échoué) dus à un cyberincident.

Les exploitants de terminaux portuaires et les agents maritimes tendent à contrôler les systèmes informatiques et de TO liés au mouvement des marchandises. Le degré d'interconnectivité entre ces systèmes engendre des risques supplémentaires qui font que les agents maritimes et les transporteurs de fret ont été pris pour cible lors d'opérations de piratage psychologique. De fait, de nombreux exploitants de terminaux ont été considérés comme l'épicentre des attaques de cybersécurité dans de nombreux ports du monde entier et au Canada[8]. Les cyberattaques contre les terminaux portuaires sont très perceptibles, car elles créent un retard supplémentaire dans les chargements et les déchargements et entraînent l'arrêt des opérations.

Pour ce qui est des exploitants de navires, les chargeurs canadiens ont indiqué qu'ils souhaitaient que le gouvernement prenne des mesures incitatives pour renforcer la cybersécurité dans le secteur maritime. Des mesures incitatives peuvent être établies pour persuader les entreprises à effectuer des essais d'hameçonnage, à former leurs employés, à

souscrire une meilleure cyberassurance, à migrer leurs données vers le nuage, à adopter des normes comme la CMMC et à se faire accréditer. Les spécialistes de la cybersécurité du CCC proposent des services gratuits, des alertes d'information sur la cybersécurité et des appels toutes les deux semaines à l'ensemble du secteur des transports. De plus, Sécurité publique Canada aide les propriétaires d'infrastructures essentielles à accroître leur résilience en organisant des symposiums, des ateliers et des exercices sur table.

Comme l'ont souligné certains universitaires au cours des discussions, une grande part du débat actuel se concentre trop sur le court terme – les rançongiciels et les problèmes génériques de cybersécurité pour lesquels il existe des solutions – et ne se concentre pas sur les événements de type « cygne noir » qui concernent les TI, les TO et les opérations[9]. Les universitaires ont noté que le gouvernement doit envisager les pires scénarios, afin que les propriétaires et exploitants puissent commencer à élaborer une feuille de route prospective. Les solutions doivent suivre l'évolution des menaces et des dangers.

La planification et la simulation des prochains défis en matière de cybersécurité au moyen d'exercices sur table regroupant l'industrie et le gouvernement préparent le secteur maritime aux cyberattaques inévitables ainsi qu'aux risques secondaires comme la recherche et sauvetage, la lutte contre la pollution et l'abordage. Ces exercices sur table permettent de créer de possibles cadres de cyberrisque maritime et des matrices des menaces visées par les autorités portuaires canadiennes (APC) et les experts en cybercriminalité maritime. En outre, les exercices sur table ont l'avantage d'aider le secteur maritime à comprendre à quel risque il est exposé, et dans quelle mesure.

Questions et recommandations

Les questions et recommandations suivantes s'inspirent des observations et des discussions collaboratives qui ont eu lieu lors de la Journée de l'industrie. Par conséquent, elles sont présentées sans que les parties prenantes participant à l'événement soient identifiées.

Formation à la cybersécurité maritime

Il est nécessaire de combler le fossé entre les spécialistes en information, les spécialistes en opérations et les exploitants du secteur maritime. En d'autres termes, ces trois communautés ne parlent pas le même langage, et n'ont pas les mêmes priorités. Il est absolument nécessaire de commencer dès aujourd'hui à former la main-d'œuvre qui fera face aux problèmes de demain. Ce processus doit commencer le plus tôt possible, car il faut souvent de cinq à six ans pour former entièrement le personnel dans un secteur particulier. Il est donc impératif de former une nouvelle génération de spécialistes qui connaissent les trois volets : cybersécurité, SCI et opérations. Il est nécessaire que les parties prenantes du secteur maritime restent tournées vers l'avenir pour faire face aux problèmes de demain. Les agents de confiance qui entrent dans les ports constituent un autre vecteur d'attaque. De nombreuses entreprises, entrepreneurs et visiteurs peuvent ne pas avoir le même niveau de formation à la cybersécurité (comme la cyberhygiène) que le personnel portuaire. Un exercice sur table peut aider à se préparer à des conditions simulées futures et favoriser la résilience.

Recommandations

- Continuer à travailler aux échelons interministériel et international pour évaluer les modèles éducatifs qui sont reconnus par l'OMI et par les sociétés de classification internationales. Ces efforts contribueront à assurer l'élaboration de normes de formation de base obligatoires en matière de sécurité pour les équipages qui interagissent avec les systèmes de TO et de TI.

- Poursuivre le dialogue interministériel afin d'explorer des possibilités de mettre en place, au sein du gouvernement fédéral, des stages en cybersécurité qui mettent l'accent sur le secteur maritime.

- Prendre l'engagement, à l'échelle interministérielle, de veiller à ce que le secteur maritime soit mentionné de manière appropriée dans le Plan d'action sur la cybersécurité.

- Les propriétaires de navires, les ports et les exploitants de terminaux portuaires sont encouragés à travailler avec des entreprises de cybersécurité maritime et (ou) des sociétés de classification afin d'améliorer leur profil de cybersécurité pour ce qui est des contrôles de sécurité appliqués et des systèmes qui se trouvent dans leur champ d'application, et d'analyser les ateliers et les formations proposés par SPC et le CCC.

- S'engager à l'échelle interministérielle et, éventuellement, avec l'industrie, à planifier ou à tirer parti d'un exercice sur table existant pour simuler une éventuelle cybermenace dans un environnement maritime.

Financement de la cybersécurité maritime

Toute forme d'amélioration des niveaux de cybersécurité pour les autorités non portuaires nécessitera des investissements importants en matière de ressources financières et humaines de la part du gouvernement. TC est à l'heure actuelle propriétaire de 19 ports distants et de quelques-uns des 31 ports régionaux parmi les 550 ports publics. Il est nécessaire de moderniser les infrastructures portuaires vieillissantes et obsolètes, et les parties prenantes cherchent à demander au gouvernement fédéral de créer une politique de cybersécurité qui vise non seulement les autorités portuaires, mais aussi les ports de petite et moyenne taille.

Afin de mettre en évidence cette interconnexion, une étude de cas simulée a été menée en 2019 par le *Cambridge Centre for Risk Studies* pour examiner les répercussions possibles d'un virus informatique transmis par les navires aux ports connectés. Dans l'un des scénarios les plus pessimistes, le virus a détruit la base de données des marchandises de 15 ports d'Asie et causé des dommages s'élevant à 110 milliards de dollars, dont 101 milliards ne seraient pas assurés[10]. Cette étude de cas met en évidence les vulnérabilités d'une infrastructure portuaire essentielle vieillissante dans une région où l'interconnexion est très rapide. Si un auteur de menace est incapable d'accéder au serveur du port, il essaiera de compromettre un locataire qui a un accès de confiance au réseau du port.

Recommandations

- Poursuivre les travaux en vue de relever les possibilités de financement nouvelles et existantes dans le domaine de la cybersécurité maritime, y compris les initiatives public-privé.

Atténuation des perturbations des systèmes de positionnement, de navigation et de synchronisation

Les dispositifs de brouillage (générateurs d'interférences ou suppresseurs de signaux) sont interdits au Canada. Les problèmes liés aux perturbations des systèmes de positionnement, de navigation et de synchronisation (PNS) pourraient avoir d'énormes répercussions sur le secteur maritime, notamment sur les opérations de transport maritime. Les problèmes de brouillage et d'usurpation du système de positionnement global (GPS) et des systèmes d'identification automatique (SIA) sont bien documentés depuis de nombreuses années, et les perturbations découlant d'une perte de signal sont amplifiées dans l'espace confiné d'un port. Selon les

universitaires du Conseil de l'Atlantique : « les SIA sont parmi les systèmes les plus essentiels de l'industrie maritime, car ils permettent l'échange d'alertes sur le positionnement et l'information des navires… les effets éventuels d'une compromission [du positionnement, de la navigation et de la synchronisation] sont importants, car les navires modernes dépendent fortement de ces systèmes satellitaires et radio pour la navigation ». [Traduction libre][11] Les attaques visant les systèmes de navigation peuvent avoir des effets perturbateurs individuels (p. ex. retarder l'arrivée au port d'un seul navire) ou des effets perturbateurs globaux (notamment provoquer l'échouage d'un navire, le blocage d'un port ou d'une voie navigable pendant plusieurs jours ou plus).

La Garde côtière est le principal propriétaire et exploitant des SIA et d'autres infrastructures maritimes essentielles au Canada. L'une des plus importantes cybermenaces est celle qui pèse sur les SIA et les autres systèmes de navigation. L'usurpation du système GPS est devenue si courante dans certaines régions du monde que beaucoup considèrent que le système n'est pas fiable et ont fréquemment recours à d'autres moyens de navigation.

Recommandations

- Étudier les options (autorités, technologies) pour détecter, combattre et atténuer les effets du brouillage et de l'usurpation du SIA et du GPS dans les voies navigables du Canada[12].

Mise en commun de l'information

Les renseignements sur les cyberrisques maritimes sont une exigence essentielle qui soutient directement une prise de décisions raisonnées et en temps opportun. Cette réalité souligne l'importance de la mise en commun de l'information et de la protection des renseignements en temps utile parmi les partenaires. Or, le signalement des cyberincidents touchant les ports et les navires n'est pas obligatoire au Canada, sauf lorsqu'il s'agit d'une violation de la *Loi sur la protection des renseignements personnels et les documents électroniques*. En fait, de nombreuses entreprises du secteur maritime craignent que le signalement d'information sur l'incident qu'ils ont subi ne nuise à leur réputation. La mise en commun d'information sur les incidents de cyberrisques peut aider à déterminer le risque réel dans ce secteur, surtout si les organismes qui reçoivent l'information sur un incident disposent d'un solide programme de divulgation garantissant l'anonymat, comme le mécanisme de signalement du CCC.

Recommandations

- La Garde côtière continuera à organiser annuellement la Journée de l'industrie sur la cybersécurité maritime afin de promouvoir la résilience en matière de cybersécurité et la mise en commun de l'information entre le gouvernement et ses partenaires de l'industrie.

- Évaluer la meilleure façon d'établir une relation avec le *US Maritime Transportation System Information Sharing Analysis Centre* (MTS-ISAC), en tenant compte du modèle de participation fondé sur l'abonnement. Le MTS-ISAC propose, aux parties prenantes des infrastructures maritimes essentielles, un service de mise en commun de l'information qui tient lieu de point de coordination centralisé afin de permettre l'échange de renseignements sur les cybermenaces à jour et exploitables entre parties prenantes de confiance.

- Continuer à favoriser la confiance de l'industrie et du milieu universitaire afin de faciliter le partage de pratiques exemplaires et de faire progresser le débat autour de la cybersécurité du secteur maritime et, ainsi, de permettre la mise au point de cybersolutions conjointes.

- Étudier les méthodes qui permettent d'améliorer la diffusion de renseignements sur les cyberrisques auprès des parties prenantes du secteur maritime lors des situations d'urgence et non urgentes.

La cybersécurité maritime dans les chaînes d'approvisionnement

Le secteur maritime est une industrie interconnectée qui nécessite une connaissance globale des besoins des principales parties prenantes et des risques auxquels elles peuvent s'attendre dans la mesure où elles ne sont pas des spécialistes de la cybersécurité. Or, l'inaction ouvre la porte aux auteurs malveillants désireux d'exploiter les vulnérabilités. Une entreprise de cybersécurité a mené une enquête auprès du secteur maritime; on comptait parmi l'échantillon utilisé pour l'enquête des marins, des responsables dans les ports et des fournisseurs. L'enquête a permis de constater que les armateurs ne demandent qu'à 55 % des fournisseurs du secteur de prouver qu'ils ont mis en place des procédures de gestion des cyberrisques. Lors de la mise en service d'équipement maritime, l'organisme acquéreur a, par défaut, peu de

difficulté à y accéder. Dans certains cas, les fabricants peuvent intégrer à l'équipement un niveau de sécurité approprié qui répondra aux besoins de l'organisme. Cependant, ce ne sont pas tous les organismes qui demandent ces ajouts de sécurité, si bien que cet équipement, facilement accessible, devient une source de vulnérabilités en matière de cybersécurité. Il est préférable que les fabricants d'équipement d'origine (FEO) créent des produits qui intègrent le principe de la sécurité dès la conception, ce qui peut nécessiter la normalisation d'un produit et de mener des essais d'intrusion grâce à des micrologiciels.

Recommandations

- Dans la mesure du possible, il est recommandé d'acquérir de l'équipement électronique et des logiciels auprès de fournisseurs qui ont adopté – ou qui sont en voie d'adopter – les normes *NIST 800-161 Supply Chain Risk Management, ISA99 Standard on Developing Products that are Cybersecure by Design*, et ISO 28000s. Dans la mesure du possible, l'équipement doit être acquis auprès de fournisseurs qui ont adopté l'accréditation CMMC ou qui sont engagés dans cette voie.

- Soutenir l'Organisation maritime internationale lorsqu'elle envisage d'élaborer des lignes directrices sur la sécurité de la conception.

Autorités chargées de la cybersécurité maritime

Lorsqu'un virus transmis par un locataire du port vient perturber les activités, un tel incident influe sur les opérations globales des autorités portuaires, vient provoquer des retards dans le chargement et le déchargement des marchandises et peut entraîner des embouteillages de navires. L'Association des administrations portuaires canadiennes a demandé plus de clarté quant aux processus de coordination et de prise de décision ainsi qu'aux pouvoirs des ministères et organismes fédéraux. Cela s'explique par les nombreuses couches de menace qui touchent particulièrement le domaine maritime, notamment les ports, les navires, les centres de contrôle du trafic maritime, les navires autonomes sans équipage et leurs systèmes informatiques et (télématiques) individuels.

Le Canada est un État signataire de l'OMI, une institution spécialisée des Nations Unies responsable des mesures visant à améliorer la sécurité et la sûreté de la navigation internationale et à prévenir la pollution par les navires. Conformément aux directives de l'OMI sur la gestion des cyberrisques maritimes, les ports doivent également adopter une approche tous risques de la cybersécurité maritime en intégrant les cyberrisques dans leurs plans de

continuité des activités. Une approche tous risques est nécessaire dans ce secteur essentiel de l'infrastructure de transport afin de renforcer la capacité à répondre aux menaces et à empêcher les dangers de devenir des catastrophes.

Recommandations

- En tant que communauté, il est nécessaire de continuer à élaborer une voie à suivre sur cet aspect de la conversation, en poursuivant le dialogue lors de la prochaine Journée de l'industrie 2023.

Conclusion

L'engagement dans ce secteur a été à la fois concret et constructif pour ce qui est de la sensibilisation à la cybersécurité maritime et de la mise en commun de l'information. Il souligne les enjeux de la protection du secteur maritime, qui est l'un des principaux secteurs des infrastructures essentielles. Les partenaires fédéraux et l'industrie se partagent la responsabilité de cerner et de gérer les cyberrisques maritimes, et continueront à collaborer en vue d'harmoniser les approches en matière de cybersécurité maritime afin de garantir la cyberrésilience du navire à la côte.

Le cyberespace fait partie intégrante de tout ce que font le gouvernement et l'industrie, et la Journée de l'industrie sur la cybersécurité maritime concorde avec de nombreux autres documents, comme la *Stratégie nationale de cybersécurité* et la *Stratégie nationale sur les infrastructures essentielles*. Alors que la Garde côtière et d'autres organismes mettent à l'essai des systèmes maritimes autonomes, il faut être conscient qu'il s'agit d'une arme à double tranchant, riche en possibilités, mais aussi en vecteurs d'attaque qui pourraient être exploités par des acteurs malveillants à une époque de connectivité accrue.

La Garde côtière et le secteur maritime au sens large doivent participer à l'apprentissage continu dans le secteur maritime. Dans ce contexte, le gouvernement s'engage avec l'industrie pour protéger collectivement le secteur maritime et accroître la sensibilisation aux cyberrisques maritimes, l'objectif étant d'appuyer la sécurité et la sûreté du secteur du transport maritime et d'accroître sa résilience aux cyberrisques sur le plan opérationnel. La Garde côtière se réjouit de collaborer avec l'industrie, le milieu universitaire et d'autres services gouvernementaux pour continuer à faire progresser les meilleures solutions pour la protection du secteur maritime.

Annex I : Glossaire

Un **« système d'identification automatique (SIA) »** est un système de repérage automatique qui utilise des émetteurs-récepteurs sur les navires et est utilisé par les services du trafic maritime (STM) afin de prévenir les collisions sur l'eau.

Une **« menace persistante avancée »** est un adversaire qui possède des niveaux d'expertise sophistiqués et des ressources importantes qui lui permettent de créer des occasions d'atteindre ses objectifs en recourant à de multiples vecteurs d'attaque (p. ex. cyber, physique et tromperie). Ces objectifs consistent généralement à établir ou à élargir une position au sein des infrastructures de TI d'organismes ciblés afin d'exfiltrer des renseignements, de saper ou d'entraver les aspects critiques d'une mission, d'un programme ou d'un organisme, ou de se positionner pour réaliser ces objectifs à l'avenir[13].

Une **« porte dérobée »** est un moyen non documenté, privé ou peu détectable d'accéder à distance à un ordinateur, de contourner les mesures d'authentification et d'obtenir l'accès à du texte en clair.

« Infrastructures essentielles » s'entend des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services qui sont essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens, ainsi qu'au fonctionnement efficace du gouvernement. Il peut s'agir d'infrastructures autonomes, interconnectées ou interdépendantes au sein d'une province ou d'un territoire, entre des provinces et des territoires et à l'échelle nationale ou entre plusieurs pays. Il existe dix secteurs d'infrastructures essentielles : énergie et services publics; finances; alimentation; transport; gouvernement; technologies de l'information et des communications; santé; eau; sécurité; et fabrication.

Une **« cyberattaque »** est l'utilisation de moyens électroniques pour interrompre, manipuler, détruire ou obtenir un accès non autorisé à un système, un réseau ou un dispositif informatique.

Un **« cyberincident »** est toute tentative non autorisée, qu'elle soit réussie ou non, d'accéder, de modifier, de détruire, de supprimer ou de rendre indisponible un réseau informatique ou une ressource du système.

« Cybersécurité » s'entend de la protection des renseignements numériques ainsi que de l'intégrité de l'infrastructure qui héberge et transmet les données numériques. Plus précisément, la cybersécurité comprend l'ensemble des technologies, des processus, des pratiques et des mesures d'intervention et d'atténuation conçus pour protéger les réseaux, les ordinateurs, les

programmes et les données contre les attaques, les dommages ou les accès non autorisés, afin de garantir la confidentialité, l'intégrité et la disponibilité.

« Cybermenace » s'entend de l'action d'un auteur malveillant qui, en recourant à Internet, profite d'une vulnérabilité connue dans un produit dans le but d'exploiter un réseau et les renseignements que ce dernier transporte.

Les **« centres d'échange du renseignement et de l'information (CERI) »** sont des organismes sans but lucratif qui fournissent une ressource centrale pour la collecte d'information sur les cybermenaces, dans de nombreux cas pour les infrastructures essentielles, et qui permettent l'échange bidirectionnel de renseignements entre le secteur privé et le secteur public sur les causes profondes, les incidents et les menaces, ainsi que le partage d'expériences, de connaissances et d'analyses[14].

Les **« systèmes de technologie de l'information (TI) »** désignent l'application des ressources de réseau, de stockage et d'ordinateur à la production, à la gestion, au stockage et à la transmission de données au sein d'organismes et à travers ceux-ci. En termes plus simples, les systèmes de TI gèrent le flux d'information numérique grâce à l'utilisation de composants comme les applications commerciales, les données, le matériel (par exemple, les ordinateurs, les serveurs physiques et les équipements de réseau) et les logiciels (par exemple les applications, les systèmes d'exploitation et les capacités de virtualisation). Les systèmes de TI ont une capacité programmable, de sorte qu'ils peuvent être ajustés, enrichis et reprogrammés d'innombrables façons pour s'adapter à l'évolution des réseaux, des applications et des besoins des utilisateurs.

L'**« Organisation maritime internationale (OMI) »** est l'organisme spécialisé des Nations unies chargé de la sécurité et de la sûreté de la navigation et de la prévention de la pollution marine et atmosphérique par les navires[15].

Un **« maliciel »** (*malware*) est un logiciel malveillant conçu pour infiltrer ou endommager un système informatique, sans le consentement de son propriétaire. Les formes courantes de logiciels malveillants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.

Les **« cyberrisques maritimes »** désignent dans quelle mesure un actif technologique pourrait être menacé par une circonstance ou un événement éventuel, qui pourrait entraîner des défaillances opérationnelles, de sécurité ou de sûreté reliées au transport maritime en raison de l'altération, de la perte ou de la compromission de renseignements ou de systèmes.

Cyberespace maritime : Le « cyberespace maritime » est un domaine mondial constitué de réseaux interdépendants de systèmes de TI, de systèmes de TO, d'Internet, de données, du spectre électromagnétique (SEM) et de réseaux de télécommunications utilisés dans le domaine maritime à bord des navires et dans les ports.

Les systèmes de **« technologie opérationnelle »** (TO) font renvoi aux technologies de surveillance et de contrôle de dispositifs et de processus précis dans les flux de travail industriels. Ces systèmes exécutent la fonction de processus physiques par l'intermédiaire de matériel et de logiciels qui sont généralement conçus pour exécuter des fonctions précises, par exemple contrôler la chaleur, surveiller les performances mécaniques, déclencher des arrêts d'urgence, etc. En général, cela se fait par l'intermédiaire du SCI et du système de contrôle et d'acquisition de données (SCADA).

Les **« correctifs »** sont des mises à jour de logiciels et de systèmes d'exploitation qui corrigent les failles de sécurité d'un programme ou d'un produit. Les fournisseurs de logiciels peuvent choisir de publier des mises à jour pour corriger des bogues de performance, ainsi que pour fournir des fonctions de sécurité améliorées.

Le **« hameçonnage »** (*phishing*) est une tentative par un tiers de solliciter des renseignements confidentiels auprès d'une personne, d'un groupe ou d'un organisme en imitant ou en usurpant une marque, généralement bien connue, généralement dans un but financier.

Les systèmes de **« positionnement, de navigation et de synchronisation (PNS) »** sont utilisés pour aider à comprendre où se trouvent les navires sur la surface de la Terre (positionnement), pour déterminer comment se rendre là où le navire doit aller (navigation), et pour synchroniser les réseaux ou pour l'horodatage.

Les **« perturbations des systèmes PNS »** se rapportent au brouillage ou à l'usurpation des systèmes PNS.

- Le brouillage suppose un dispositif de brouillage des radiocommunications, également connu sous le nom de silencieux, bloqueur ou désactivateur de signal, et conçu pour interférer avec, perturber ou bloquer les signaux et services de radiocommunication.

- L'« usurpation » (*spoofing*) consiste à se faire passer pour une personne ou une entreprise afin d'accéder à des renseignements délicats ou de diffuser des logiciels malveillants. Elle peut s'appliquer à diverses voies de communication et peut supposer

différents degrés de complexité technique. La mystification par GPS utilise de faux signaux qui sont diffusés pour tromper la victime. Par exemple, un récepteur de navire peut être trompé par des signaux d'identification automatique de satellite contrefaits émis pour prendre le contrôle du système de navigation en faisant dévier le navire de sa route ou le faisant apparaître à un endroit différent.

La **« sécurité dès la conception »** renvoie à la sécurité qui est intégrée dans l'architecture technique de tout ce qui est créé et devrait donc être intégré dans les cycles de vie futurs.

Les **« sociétés de classification des navires »** sont des organismes non gouvernementaux qui fixent et appliquent des règles de conception et de construction afin de garantir que les structures des navires et que leurs constructeurs respectent ces règles. Leur mandat consiste à évaluer les nouveaux navires sur la base de normes techniques prédéfinies, puis à leur attribuer une « classe » en fonction de leur conception. Les sociétés de classification offrent également d'autres services, comme des inspections et des visites de navires pour le compte d'autorités gouvernementales, afin de garantir le respect des règlements.

Notes de bas de page

[1] Conseil des académies canadiennes, *La valeur du transport maritime commercial pour le Canada. Ottawa (Ontario) : le comité d'experts sur la valeur sociale et économique du transport maritime commercial pour le Canada.* 24 mai 2017. La valeur du transport maritime pour le Canada | Clear Seas (Consulté le 24 mars 2022)

[2] CyberOwl, *HFW Report : Maritime Industry Pays Average $3m Ransom in Cyberattacks*. 22 mars 2022. CyberOwl, HFW Report: Maritime Industry Pays Average $3m Ransom In Cyberattacks - Cyber Owl (rapport en anglais seulement, consulté le 25 mars 2022)

[3] De nombreux chargeurs et chantiers navals ont été touchés par d'importantes cyberattaques. Nous croyons savoir qu'ils disposent désormais de structures beaucoup plus robustes de réponse aux cyberincidents. En voici une liste non exhaustive : 2022 Expeditors International, États-Unis; 2021 Bureau Veritas, France; 2021 Swire Pacific Offshore, Singapour; 2020 Chantier naval de Vard, Norvège; 2020 Compagnie Maritime d'Affrètement (CMA) et Compagnie Générale Maritime (CGM), France; 2020 Mediterranean Shipping Company, Suisse; 2018 Constructeur naval Austal, Australie; 2017 Maersk Shipping, Danemark; 2017 Courtier maritime Clarksons, Royaume-Uni.

[4] Aux États-Unis, les membres de la Chambre des représentants ont présenté la *Port Crane Security and Inspection Act of 2022* (loi de 2022 sur la sécurité et l'inspection des grues portuaires), qui limite l'exposition au risque de cybersécurité dans leur secteur d'infrastructures maritimes essentielles en matière de cybersécurité, détenues ou fabriquées par des pays étrangers. Pour de plus amples renseignements, prière de consulter la *Port Crane Security and Inspection Act of 2022* (en anglais seulement). Le Congrès américain sur le Web. Le 26 janvier 2022. https://www.congress.gov/bill/117th-congress/house-bill/6487/text?r=18&s=1 (consulté le 5 avril 2022).

[5] Deborah Haynes, *Iran's Secret Cyber Files: How Cargo Ships Could be Sink* (en anglais seulement). Sky News sur le Web. 27 juillet 2021. https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871 (consulté le 25 mars 2022).

[6] Daphne Leprince-Ringuet, "The Global Chip Shortage is Creating a New Problem: More Fake Components," ZDNet on the Web. June 9, 2021. https://www.zdnet.com/article/the-global-chip-shortage-is-creating-a-new-problem-more-fake-components-as-fraudsters-cash-in/ (consulté le 27 mars 2022).

[7] International Association of Classification Societies, *IACS Adopts New Requirements on Cyber Safety* (article en anglais seul.) 21 avril 2022 IACS adopts new requirements on cyber safety - IACS (consulté le 17 octobre 2022)

[8] La liste non exhaustive ci-après fournit des exemples de ports ou de terminaux portuaires qui ont été victimes de cyberattaques : 2022 : Terminal à conteneurs Jawaharlal Nehru, Inde; 2021 : Port de Houston, États-Unis; 2021 : Port de Le Cap, Port d'Elizabeth et Durban, Port de Ngqura, Afrique du Sud; 2020 : Port de Kennewick, États-Unis; 2020 : Port de Shahid Rajee, Iran; 2020 : Port de Marseille, France; 2018 : Port de Vancouver, Canada; 2018 : Port de San Diego, États-Unis; 2018 : Port de Barcelone, Espagne; 2018 : Transport maritime COSCO au port de Long Beach, États-Unis; 2017 : Port de Rotterdam, Pays-Bas.

[9] Dans une enquête menée par une société de cybersécurité maritime, plus de 25 % des marins ne savent pas quelles mesures on leur demanderait de prendre en cas de cyberincident. Pour plus de plus amples renseignements, prière de consulter le rapport CyberOwl, HFW : *Maritime Industry Payout Average $3m Ransomware Cyberattacks* (L'industrie maritime paie en moyenne 3 millions de dollars pour les cyberattaques de type rançongiciel – article en anglais seulement). *CyberOwl sur le Web*. Le 22 mars 2022.https://cyberowl.io/cyberowl-hfw-report-maritime-industry-pays-average-3m-ransom-in-cyberattacks/ (consulté le 1er avril 2022).

[10] J. Dafrron et coll., Shen Attack : Cyber Risk in Asia Pacific Ports, Cambridge Centre for Risk Studies, 2019, https://assets.lloyds.com/assets/pdf-cyrim-shen-attack-final-report-exec-summary/1/pdf-cyrim-shen-attack-final-report-exec-summary.pdf (consulté le 18 janvier 2022).

[11] A System of systems: Cooperation on Maritime Cybersecurity, Atlantic Council on the Web (en anglais seulement). 4 octobre 2021. https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-a-system-of-systems/ (Accessed on Jan 11, 2022).

[12] Il importe d'harmoniser les définitions dans le domaine de la cybersécurité. Le 2 mars 2022, le US committee of National Security Systems définit le cyberespace maritime comme suit : « Le cyberespace maritime est un domaine mondial constitué des réseaux interdépendants de l'infrastructure des technologies de l'information (TI), de l'infrastructure des technologies opérationnelles (TO), d'Internet, des données résidentes, du spectre électromagnétique (EMS) et des réseaux de télécommunications, des ordinateurs, des systèmes d'information et de communication, des processeurs intégrés et des contrôleurs liés aux processus et fonctions de l'infrastructure ». [Traduction libre]

[13] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf pg H-4

[14] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[15] https://www.imo.org/fr