Les ports, nouvel enjeu de la cyber résilience de la chaine d'approvisionnement logistique !

Jérôme BESANCENOT
Directeur de projet transition numérique
HAROPA PORT

Le secteur portuaire : une interdépendance mondiale face au risque cyber

Les différentes et récentes crises internationales (Covid, Ever Given, conflit en Ukraine) ont illustré de manière diverse la fragilité de nos chaines d'approvisionnement et l'importance des ports pour garantir le ravitaillement des nations.

Ces crises génèrent des désorganisations chroniques dans les chaines logistiques qui peinent à revenir à leur vitesse de croisière du fait de pénuries sur certaines matières premières et de congestions portuaires faisant suite à une reprise soutenue des exportations.

Ces congestions induisent des difficultés de planification des escales dans les ports et notamment dans le fonctionnement des opérateurs terminaux qui font face à de très forts surcroits d'activité.

Les ports entrainés dans cette spirale doivent recourir à des outils numériques toujours plus sophistiqués pour préparer l'arrivée des navires, assurer leur navigation en sécurité, synchroniser les actions des différents acteurs intervenant sur les opérations portuaires et faciliter le passage des marchandises en interconnexion avec les acteurs du pré post acheminement.

L'usage de données numériques massives comme le Big Data, les développements de nouveaux services à valeur ajoutée grâce à l'Intelligence Artificielle (IA), le « deep learning », l'IoT ou des moyens de communication toujours plus puissant comme la 5G, conduisent les ports à se doter d'environnements virtuels comme les jumeaux numériques (Digital Twin), pour optimiser leurs activités toujours plus complexes et s'adapter rapidement aux enjeux économiques, politiques et environnementaux.

Cette accélération numérique vertigineuse s'inscrit dans une exigence pour les ports, d'offrir une meilleure qualité de services à leurs clients notamment en garantissant une traçabilité complète sur les marchandises, leurs statuts et les moyens de transport au bénéfice d'une chaine d'approvisionnement plus performante et qualitative. Cette volonté pousse ainsi les ports à s'intégrer toujours plus loin avec les outils numériques des logisticiens, en ouvrant en particulier leurs interfaces applicatives pour systématiser les interconnexions nécessaires aux échanges d'informations.

Depuis quelques années, la cybersécurité portuaire et maritime est devenue un enjeu majeur qui interroge l'ensemble des organisations internationales sur la nécessité d'assurer une cyber résilience globale du commerce maritime, et en

particulier la cyber résilience de la chaine d'approvisionnement. Dans ce contexte, les ports devenant tributaires de la sophistication de leurs outils numériques, deviennent des maillons cyber sensibles de la logistique.

En effet les acteurs ne peuvent plus travailler seulement en silo, il est nécessaire d'intégrer le risque cyber avec une vision élargie des processus d'activités et leur criticité. Les ports ne doivent plus considérer que le risque cyber n'est qu'affaire de stratégie individuelle, il faut adresser ce risque collectivement. Un port lourdement impacté par une crise cyber va engendrer inévitablement des désorganisations d'escales sur les autres ports auxquels il est connecté, voire un risque de propagation de la cybermenace via les systèmes et données partagés entre les parties prenantes.

Le risque cyber se dissémine au-delà des organisations ou des Etats, la chaine d'approvisionnement est un réseau propice à la circulation de la menace. Un port ne pouvant être considéré comme « étanche », il faut donc bien renforcer la cybersécurité de l'ensemble des ports.

L'IAPH (Association Internationale des Ports) a souligné récemment au travers d'un guide spécifique[1] sur la cybersécurité portuaire l'ampleur de ce nouveau risque mondial, où certains ports accélèrent leur numérisation au détriment de la prise en compte du risque cyber, pouvant ainsi conduire à une fracture entre des ports mieux armés et ceux qui resteront ultra vulnérables.

Pour construire une cyber résilience globale, il est légitime pour chaque port de se pencher d'abord sur sa propre résilience, toutefois il est primordial d'être attentif à favoriser aussi la sécurité des ports auxquels il est relié, et ainsi contribuer au maintien du bon fonctionnement de la chaine d'approvisionnement logistique mondiale.

Cette considération élargie n'est pas simple à mener, car l'activité mondiale du commerce maritime est assurée par une succession d'acteurs, de nombreux systèmes hétérogènes interconnectés et des données massives transitant au travers de ces systèmes et applications, constituant plutôt une toile de systèmes qu'un système unitaire homogène. En poussant ce raisonnement, il devient presque illusoire de vouloir maitriser et identifier globalement l'ensemble de ces actifs. Cela revient un peu à faire face à une architecture informatique, dont personne ne peut maitriser la vision d'ensemble et donc les risques qui pourraient survenir.

Comment s'organiser mondialement pour renforcer globalement la cybersécurité portuaire ?

Les cyberattaques contre les ports sont souvent perturbatrices et coûteuses. Elles peuvent générer des dégâts matériels en perturbant les processus métiers mais aussi des dégâts immatériels en perturbant le fonctionnement des systèmes numériques IT ou OT.

Ces perturbations peuvent même affecter le fonctionnement d'un pays et entraîner des répercussions politiques et économiques majeures.

Les dirigeants d'entreprises portuaires, d'installations portuaires ou de ports doivent prendre en compte la gestion des risques cyber au premier niveau, et définir une stratégie de résilience pour maintenir des conditions de fonctionnement opérationnel.

Sur le plan international, il existe dorénavant des guides et des méthodes pour aider les ports à progresser et à s'organiser pour traiter les menaces cyber. L'ENISA[2] (Agence européenne chargée de la sécurité des réseaux et de l'information), l'IAPH avec

[1] IAPH Cybersecurity Guidelines for Ports and Port facilities Version 1.0 (2021)

[2] Port Cybersecurity : Good practices for the Maritime Security (2019)

l'OMI (Organisation Maritime Internationale) proposent ainsi des outils méthodologiques qui permettent aux dirigeants de travailler sur ce sujet avec efficience et de se concentrer sur des étapes clés favorisant une montée en charge rapide : identification des risques et vulnérabilités, les parties prenantes, les systèmes informatiques et industriels, l'importance des données, etc.

La notion d'opérateur de services essentiels proposée par la directive NIS de l'Union Européenne amène un premier niveau d'incitation des ports à travailler globalement à l'échelle internationale sur le sujet et à suivre une certaine méthodologie, notamment pour identifier le caractère critique d'un système numérique et définir un plan d'action au regard des risques inhérents. L'OMI réfléchit aussi pour qu'au niveau mondial, le cyber risque soit désormais appréhendé sous l'angle de la conformité. Cela a conduit à l'évolution en 2021 pour les navires du code ISM, et fait l'objet de réflexions autour du code de sûreté ISPS pour une prise en compte par les ports d'une politique de cybersécurité plus affirmée.

Néanmoins, ces différents guides ne peuvent adresser toutes les particularités des systèmes et des risques associés. Afin de garantir aux ports dans l'avenir une interconnexion et une interopérabilité mondiales accrues et sécurisées, il convient de travailler en premier lieu sur les systèmes communautaires portuaires qui assurent les échanges d'informations au niveau local pour une communauté ou au niveau international pour le commerce maritime.

Un premier sujet d'investigation porte donc légitimement sur les systèmes communautaires informatiques dits PCS (Port Community System) qui restent la véritable pierre angulaire de l'organisation prévisionnelle et opérationnelle de l'escale, son suivi, et du passage des marchandises et des passagers. Ces outils sont également la source principale des données numériques utilisées par les jumeaux numériques portuaires.

Ces systèmes assurent un fonctionnement optimisé du port sur le plan opérationnel mais aussi administratif. Sur ce dernier volet, les PCS jouent un rôle essentiel pour faciliter la transmission des informations réglementaires obligatoires aux Guichets Uniques (GU) maritimes ou douaniers de chaque Etat. Ces derniers sont des instruments fondamentaux dans la facilitation du commerce international et de la sécurité du transport par voie maritime. De fait, les PCS et les GU offrent une interconnexion et une interopérabilité accrues entre les acteurs du transport maritime, et la réutilisation de données massives électroniques.
Les PCS gèrent des milliers de connexions et échangent des millions d'informations. Ils sont reconnus comme des outils référents nécessaires à l'interfaçage du monde maritime, portuaire et logistique. Leur forte expansion dans les ports (voire aéroports) démontre leur pertinence pour la chaine d'approvisionnement.

La cybersécurisation globale des systèmes portuaires, un enjeu de résilience et de souveraineté

Les PCS sont principalement développés par des sociétés de services informatiques ou par des autorités portuaires. Ils permettent d'automatiser, de sécuriser, de fluidifier les processus métiers liés aux escales ou aux marchandises, et sont les traits d'union avec les chargeurs, les commissionnaires de transport, les opérateurs de terminaux, les

Cyber Risk Management for Ports (2020)

compagnies maritimes et les plateformes logistiques multimodales qui utilisent les ports. Ils jouent un rôle majeur dans la chaine de valeur au titre des importations et exportations.
Pour cette raison, il parait important d'orienter les travaux de cybersécurité sur le rôle et la place de ces systèmes dans les écosystèmes portuaires, d'avoir un regard à 360° pour examiner l'existence de menaces cyber et anticiper les risques relatifs.

Un travail préalable doit porter sur les interfaces et interconnexions des PCS avec les systèmes des acteurs portuaires, maritimes ainsi que les GU. L'objectif est clairement de sécuriser les échanges de données en sanctuarisant certains canaux de connexion (emails, interfaces hommes machines, EDI, API etc.). Ces derniers restent encore très diversifiés et reposent trop souvent sur des protocoles plus ou moins sécurisés. L'idée ici est d'harmoniser les méthodes d'échanges en tenant compte du caractère de sensibilité de l'information et l'importance de sa disponibilité. Il serait illusoire et coûteux de vouloir tout surprotéger, il faut aussi considérer les capacités technologiques, la complexité des solutions et la capacité des acteurs à les mettre en œuvre. Autrement dit, éviter de compliquer l'organisation des clients avec des solutions complexes et contraignantes quand cela n'est pas nécessaire. L'important est d'assurer une démarche progressive et ciblée en fonction des besoins et des risques associés. Généralement, les échanges peuvent s'appuyer sur des réseaux privés virtuels (VPN) entre acteurs qui se connaissent et échangent régulièrement des informations. Ces solutions ne sont malheureusement pas toujours adaptées quand les acteurs échangent de manière plus sporadique. Comment maintenir l'accès aux PCS sans imposer systématiquement une protection additionnelle délicate. Les PCS évoluent et intègrent de plus en plus ces composantes au sein de leur offre de service pour sécuriser les clients graduellement en fonction de leurs besoins. Il convient à présent de normer plus formellement ces services en fonction de la nature des échanges, afin de partager ces bonnes pratiques entre les ports.

Un autre axe de travail doit utilement s'orienter sur les données dites essentielles à l'activité portuaire. Pour sécuriser les systèmes au-delà des interfaces, une approche complémentaire porte sur l'accès à la donnée elle-même qui doit faire l'objet d'une stratégie de renforcement plus poussée selon la nature sensible de la donnée, avec notamment des mécanismes de vérification de l'identité numérique de l'accédant et de ses droits d'accès assortis. Comment s'assurer que ces données restent suffisamment sécurisées pour être utilisées sans risque dans des activités sensibles tel le guidage du navire et sa mise à quai ? Les PCS s'appuient toujours davantage sur les outils de navigation électronique maritime fournissant des données de positionnement AIS/GNSS ou encore de bathymétrie par le biais de cartes électroniques côtières. Au-delà de la sensibilité de la donnée, il est aussi intéressant de se pencher sur sa temporalité notamment quand elle est critique mais qu'en plus elle varie fréquemment. Une fragilité potentielle peut survenir du fait d'une désynchronisation sur la valeur de la donnée entre les systèmes des acteurs. Un constat récurrent montre que certaines données électroniques sensibles, quoique partagées, sont parfois dupliquées et stockées dans chaque système des parties prenantes, afin de préserver une forme de résilience de fonctionnement quand les interfaces sont indisponibles. Cette pratique augmente les risques d'incohérence sur les données, et donc les risques de voir se propager aisément des informations corrompues volontairement ou involontairement entre les acteurs. Des technologies de contrôle sur la valeur de la donnée pourraient être profitables sur des informations critiques, obligeant par exemple une resynchronisation pour

un usage sensible. En s'inspirant de technologie telle la blockchain, on pourrait dans certains cas favoriser un contrôle renforcé de cohérence sur la dernière valeur qualifiée (hauteur sous quille, position d'un navire, tirant d'eau, profondeur d'eau, etc.).

Enfin, le dernier axe porte sur la détection d'activités frauduleuses. Les développements en matière de cyber sécurisation doivent également s'orienter vers la recherche d'opérations douteuses ou fallacieuses afin de lutter contre les trafics illicites. Les systèmes portuaires sont de plus en plus la cible de pirates cyber pour justement faciliter l'organisation de ces opérations illégales. La détection de ces activités est très difficile et peut conduire à la recherche de signaux faibles dans l'environnement direct des systèmes portuaires ou de manière très indirecte dans l'activité foisonnante de la toile internet. L'innovation à base de IA pourrait aider à favoriser des recoupements permettant aux ports de mener des investigations complémentaires, d'améliorer leur système de protection, ou encore de sécuriser davantage les usages de leurs systèmes. Ce volet aujourd'hui n'existe pas réellement, car il reste très expérimental. Il offrirait une vision additionnelle des menaces identifiées et avérées par le M-CERT national. Il s'agirait ainsi de repérer la naissance d'un risque pour le PCS particulier d'un port.

En conduisant des efforts selon plusieurs axes, il devient possible d'améliorer la cybersécurité de bout en bout de l'ensemble des données publiques ou privées qui transite dans les systèmes portuaires ou qui est échangé entre les états membres au titre des missions de sureté et sécurité du territoire.

Dans cet esprit d'amélioration de la cybersécurité portuaire, HAROPA PORT, le Grand Port Maritime de Marseille, le Port de Toulon, le Grand Port Maritime de la Guadeloupe et France PCS (SOGET et MGI) ont été lauréats en novembre 2021 de l'appel à manifestation d'intérêt « sécuriser les territoires » grâce au projet d'innovation CYSPEO (Cyber sécurisation des sYStèmes PortuairEs Opérationnels). Ce consortium offre une large expertise en matière de systèmes d'information portuaires ainsi qu'en dématérialisation des processus métiers des ports de commerce.

Le projet repose sur des démonstrateurs opérationnels illustrant la capacité à innover dans le domaine de la cybersécurité portuaire pour améliorer la sécurité des ports français et renforcer leur position comme tiers de confiance numérique au sein de la chaine d'approvisionnement. Ces démonstrateurs, une fois validés, pourront être répliqués selon les besoins sur les territoires portuaires français.

La démarche initiale sera de définir un document de Politique de Sécurité des Systèmes d'Information (PSSI) mutualisé pour l'ensemble des ports français et leur écosystème d'acteurs. Ce document général favorisera une déclinaison opérationnelle pour chaque territoire en alignement avec les orientations de la Stratégie Nationale de Cybersécurité des Secteurs Maritime et Portuaire.

Par ailleurs, le projet contribuera à l'élaboration d'un Security Operation Center (SOC) mutualisé au bénéfice des places portuaires françaises. Ce SOC pourra superviser l'ensemble des PCS utilisés par les ports français et aider à repérer des comportements anormaux précurseurs de vulnérabilités ou d'attaques cyber. Il identifiera les menaces, recherchera les marqueurs de cyberattaques et veillera de manière globale à la sécurisation des échanges d'informations entre les acteurs et places portuaires.
Ce SOC contribuera à la fourniture d'informations clés pour le M-CERT national en charge de centraliser

et de coordonner les réponses aux incidents portuaires et maritimes.

Les ports et le secteur portuaire s'organisent pour lutter contre la menace cyber en très forte augmentation. Les démarches isolées sont aujourd'hui dépassées : il s'agit de gérer un risque qui ne se limite plus aux limites territoriales ni aux frontières. L'interconnexion des outils portuaires PCS aux outils informatiques des acteurs logistiques compose une architecture informatique polymorphe difficile à sécuriser globalement. C'est grâce à la capacité à travailler collectivement entre les ports pour renforcer la sécurité des PCS et la veille sur ces outils, qu'il sera possible d'anticiper et de réagir face aux attaques cyber. Le projet CYSPEO est une première démarche qui vise à mettre en œuvre une stratégie commune et à suivre une méthodologie unifiée pour assurer une gestion de risque adaptée et pertinente face aux enjeux de cybersécurité portuaire, et ainsi contribuer au renforcement de la souveraineté de l'Etat français en matière d'approvisionnement stratégique.