Port 2 Port

Plate-forme de sécurité


Lenovo
Port Authority
North Sea Port
Together Smarter

Table des matières

L’union fait la force

Les ports belges sont des portes d’entrée sur le monde. Ils relient les personnes, les marchandises et l’industrie, mais là où ces flux se rejoignent, il existe également des risques. Aujourd’hui plus que jamais, la criminalité organisée et les menaces transfrontalières exigent une approche commune et intégrée. Plusieurs ports ont donc exprimé le souhait de regrouper les meilleures pratiques en matière de sécurité et de mettre en place une collaboration structurelle. Cette ambition commune est à l’origine de la plate-forme de sécurité Port 2 Port.

La plateforme de sécurité Port 2 Port est une initiative conjointe de Port of Antwerp-Bruges, North Sea Port et de la police fédérale CSD Limbourg, en étroite collaboration avec le Commissariat National Drogue. La plateforme, lancée le 21 novembre 2025, rassemble tous les ports maritimes et fluviaux belges. Une nouvelle étape pour rendre nos ports plus résilients dans une société en constante évolution.

Nos ports sont ouverts au commerce mondial, mais fermés à la criminalité.

Avec la nomination d’Ine Van Wymersch au poste de Première Commissaire Nationale Drogue, la Belgique dispose désormais d’un interlocuteur unique dans la lutte contre le crime organisé et la criminalité liée à la drogue. Dans le cadre de ses fonctions, elle élabore, en collaboration avec ses collègues du Commissariat National Drogue, une stratégie nationale intégrée qui rassemble la police, la justice, les ports, les entreprises et les citoyens autour d’un objectif commun : rendre notre société et nos portes économiques résistantes à l’infiltration criminelle. Cette approche a pris forme dans la stratégie de l’Iceberg.

La coopération n’est pas une option, mais une nécessité

« Nos ports sont des moteurs économiques d’envergure mondiale », déclare Ine Van Wymersch. « Ils voient défiler chaque jour des milliers de personnes, de marchandises et de navires. Cette formidable dynamique est une force, mais aussi une vulnérabilité. Les organisations criminelles tentent de s’infiltrer dans cette chaîne logistique, souvent de manière subtile, en utilisant la technologie ou en exploitant la crédulité des maillons les plus faibles. »

Selon Mme Van Wymersch, la coopération est la clé. « Personne ne peut mener ce combat seul. La police, la justice, les douanes, mais aussi les entreprises, les autorités portuaires et les syndicats doivent se concerter. Les criminels opèrent au-delà des frontières et partagent rapidement les informations. Si nous ne le faisons pas, nous courons le risque d’être dépassés par les événements. »

Elle insiste sur le fait que les bonnes pratiques et les connaissances ne doivent pas rester confinées à un seul port.
« Ce qui marche aujourd’hui à Anvers ou à Gand peut faire la différence demain dans le Limbourg, à Liège ou à Bruxelles. Nous devons partager nos connaissances, sinon nous perdrons un temps précieux. Les autorités portuaires jouent un rôle crucial à cet égard : elles font le lien entre le monde public et le monde privé. »

La stratégie de l'iceberg : tailler dans l'iceberg et réchauffer la température de l'eau

Mme Van Wymersch aime utiliser la métaphore d'un iceberg pour décrire l'approche nationale. « Les organisations criminelles sont l'iceberg. Ce que nous voyons, ce sont les saisies de drogue, les fusillades et les explosions. Mais ce n'est que la partie émergée de l'iceberg », explique-t-elle. « Sous la ligne de flottaison se joue la partie invisible, bien plus importante : blanchiment d'argent, corruption, chantage, exploitation des travailleurs. Si nous nous contentons de tailler directement l'iceberg, à partir d'une administration publique répressive, sans agir sur la température de l'eau, en renforçant la résilience des organisations et des travailleurs, il fera toujours froid dans notre écosystème. Et là où il fait froid, l'iceberg criminel ne fond pas. »

C'est pourquoi la stratégie de l'iceberg combine deux approches. « D'une part, nous avons l'approche directe : la police, la justice et les douanes qui interviennent avec fermeté (ou brisent la glace). D'autre part, nous investissons dans l'approche indirecte : prévention, formation, sensibilisation, résilience. En formant ses collaborateurs, en renforçant sa politique RH et en organisant l'échange d'informations, on réchauffe l'eau. Ainsi, l'iceberg fond et l'approche directe devient beaucoup plus efficace. »

Un écosystème, une responsabilité

Pour Mme Van Wymersch, il est clair que la sécurité ne s'arrête pas aux portes du port.

« Armateurs, terminaux, entreprises logistiques, syndicats, autorités, partenaires internationaux, tous font partie du même écosystème. Si une partie des acteurs reste en dehors de ce réseau, cela crée un espace propice à la criminalité. Ce n'est qu'en coopérant et en communiquant ouvertement que nous pourrons combler cet écart. »

Elle appelle toutes les parties concernées à ne pas attendre les autres. « L'avenir exige que nous agissions, sans attendre. Chaque autorité portuaire peut faire la différence en partageant des informations, en identifiant les risques et en utilisant la stratégie de l'iceberg comme boussole commune. Ainsi, nous faisons de nos ports non seulement des pôles économiques, mais aussi des lieux où la concurrence loyale, l'application des règles et la résilience vont de pair. »

Législation et inspections

« La loi révisée sur la sûreté maritime fait passer le standard de sécurité dans notre port à un niveau supérieur. Grâce à cette loi, nous pouvons détecter plus rapidement les risques et agir plus efficacement contre les activités criminelles. Elle nous permet de renforcer de manière structurelle la sécurité des personnes, des biens et des infrastructures. C'est essentiel pour un port fiable et tourné vers l'avenir. »

Niels Vanlaer
Président LCMB Anvers et
capitaine du port d'Anvers chez Port of Antwerp-Bruges

La sûreté portuaire n'est pas un ensemble disparate de mesures isolées, mais repose sur un cadre international solide sous la forme du code ISPS, complété par la législation nationale et des initiatives locales. Avec la loi sur la sûreté maritime, la Belgique fait partie des précurseurs en Europe dans ce domaine.

ISPS : Une norme de sûreté commune

Les bases de la sûreté maritime sont définies dans le Code international pour la sûreté des navires et des installations portuaires (International Ship and Port Facility Security - ISPS). Cette norme mondiale est obligatoire pour les navires à passagers effectuant des voyages internationaux, les navires de charge d'une jauge brute égale ou supérieure à 500 tonnes, les plates-formes de forage offshore mobiles et les installations portuaires qui accueillent ces navires.

Afin d'identifier les risques en matière de sécurité et de prendre des mesures efficaces, les évaluations de sûreté des installations portuaires et les plans de sûreté des installations portuaires sont légalement obligatoires. Il s'agit notamment des procédures relatives au contrôle d'accès, à la surveillance, à la supervision du chargement et des directives concernant les incidents et les exercices.

Outre la mise en place d'infrastructures et de procédures de sécurité, le code ISPS prévoit également un cadre pour la coopération (inter)nationale entre les acteurs publics et privés du secteur maritime.

La Belgique affiche ses ambitions avec la loi sur la sûreté maritime

Les mesures de sûreté prévues par l'ISPS ont été reprises dans le règlement européen (725/2004). La Belgique a transposé ces dispositions internationales dans sa législation nationale par le biais de la loi sur la sûreté maritime, intégrée dans le Code belge de la navigation. Cette loi utilise le cadre du code ISPS pour lutter contre la criminalité organisée, élargissant ainsi le cadre, la structure et les possibilités dont disposent les autorités publiques et les entreprises.

Cette loi a déjà fait l'objet de deux révisions, en 2022 et 2024, qui renforcent encore davantage les normes de sûreté. De cette manière, la loi offre davantage de possibilités en matière de sûreté dans les ports. Elle renforce la sûreté des ports et des installations portuaires et met l'accent sur la prévention des activités illégales telles que le trafic de drogue et la traite des êtres humains. Elle protège également les infrastructures vitales, le personnel et les installations contre toute action non autorisée.

La législation belge introduit une série de mesures innovantes qui contribuent à une approche moderne et intégrée de la sûreté :

Extrait spécial du casier judiciaire : ce nouveau document permet aux employeurs de vérifier les antécédents judiciaires des personnes qui souhaitent travailler dans le port ou dans les installations portuaires.

Interdictions de port via la plateforme AIGIS : grâce à cette plateforme, la loi prévoit la possibilité de contrôler une interdiction d'accès aux ports. Il s'agit d'une sanction pénale pour violation de la législation sur les stupéfiants et d'autres infractions pénales.

Vérifications de la sûreté via la plateforme PANOPTES : la plateforme PANOPTES rend possible la vérification obligatoire de la sûreté des personnes occupant des fonctions critiques dans le port ou les installations portuaires, telles que les personnes ayant accès à certaines entreprises, marchandises, systèmes informatiques, politiques du personnel, informations portuaires...

Utilisation de la biométrie et des caméras intelligentes : extension du cadre juridique pour le contrôle d'accès avancé et la vidéosurveillance dans le port, les installations portuaires et la partie belge de la mer du Nord.

Sécurité basée sur les risques : les terminaux fluviaux et les entreprises ayant un impact sur la sécurité maritime peuvent également être soumis à un ensemble d'exigences minimales en matière de sûreté, sur la base d'une analyse des risques.

Découvrez la plateforme AIGIS

Autorités compétentes en matière d'ISPS

La loi révisée sur la sûreté maritime garantit une approche structurelle et automatisée de la sûreté dans les ports et installations portuaires belges. La loi améliore la coopération et l'échange d'informations entre les différentes instances telles que la police locale, la DG Navigation, la Police de navigation, les douanes, la Défense, le Centre de crise national, la Sûreté de l'État, le Service Général du Renseignement et de Sécurité, l'Organe de coordination pour l'analyse de la menace, les ports (agents de sécurité portuaire), la Cellule Sûreté maritime, le Commandement provincial et les Régions.

L'Autorité nationale de sécurité maritime (ANSM), présidée par le SPF Mobilité et Transports, veille à la mise en œuvre et à l'application de la loi. Pour le suivi quotidien, l'ANSM est assistée par la Cellule Sûreté Maritime (CSM).

Dans chaque port ou voie navigable où se déroulent des activités portuaires, il existe un Comité local pour la sûreté maritime (CLSM). La Belgique compte en tout neuf CLSM. Ils coordonnent, en collaboration avec la CSM, la mise en œuvre pratique de l'ISPS dans leur zone portuaire. Un tel LCMB est une plateforme puissante et unique qui rassemble les principaux partenaires en matière de sûreté dans la zone portuaire. Grâce à son caractère local, les personnes impliquées connaissent parfaitement la région. Comme tous les participants disposent d'une habilitation de sûreté, les informations sensibles peuvent être partagées de manière sécurisée et confidentielle.

Le partage des connaissances comme levier pour la qualité

Port of Antwerp-Bruges, Rotterdam et Hambourg ont élaboré conjointement une norme commune visant à améliorer les contrôles d'accès et du périmètre ISPS. Elle permet aux autorités et aux exploitants portuaires de définir des mesures de sûreté sur la base d'une norme de risque convenue. Cette norme est désormais également obligatoire en Belgique.

Initiatives locales

Outre les normes internationales, les initiatives locales jouent un rôle important dans le renforcement de la sûreté ISPS. Un port peut donc individuellement prendre des mesures supplémentaires. Par le biais de l'ordonnance de la police portuaire, Port of Antwerp-Bruges et North Sea Port rendent obligatoires les mesures de contrôle d'accès pour toutes les entreprises situées dans la zone portuaire. Ainsi, la sûreté n'est plus limitée strictement aux sites soumis à la norme ISPS.

Dans le Limbourg, le groupe de pilotage provincial élabore actuellement une ordonnance policière similaire en collaboration avec la ville de Genk.

À North Sea Port (Gand), les lieutenants de port effectuent également des inspections ISPS intermédiaires sur la base de leur propre liste de contrôle locale. Ils utilisent pour cela une application développée en interne, qui permet une planification et un suivi structurés. À Port of Antwerp-Bruges, une équipe d'agents des autorités portuaires est prête à surveiller quotidiennement la situation et à signaler les lacunes en matière de sûreté au CLSM.

Découvrez les normes ISPS relatives à la sûreté portuaire dans cette brochure

Sites web consacrés à la sûreté

Pour plus d'informations, veuillez consulter les sites web ISPS et port security des ports belges :

Port of Antwerp-Bruges

North Sea Port

DG Navigation

Points de contact et formations

« La sensibilisation est notre première ligne de défense contre la criminalité. Il est important que nous sensibilisions toutes les personnes actives dans le port ou à proximité. Nous enseignons ainsi à nos collaborateurs et aux jeunes, grâce à des formations anti-recrutement, comment reconnaître et rejeter les tentatives de recrutement. Des points de contact tels que Portwatch facilitent ensuite le signalement anonyme de situations suspectes. C'est ainsi que nous renforçons ensemble la résilience et l'intégrité de notre port. »

Wim Van Bogaert
Président LCMB Gent et
Capitaine du port, North Sea Port

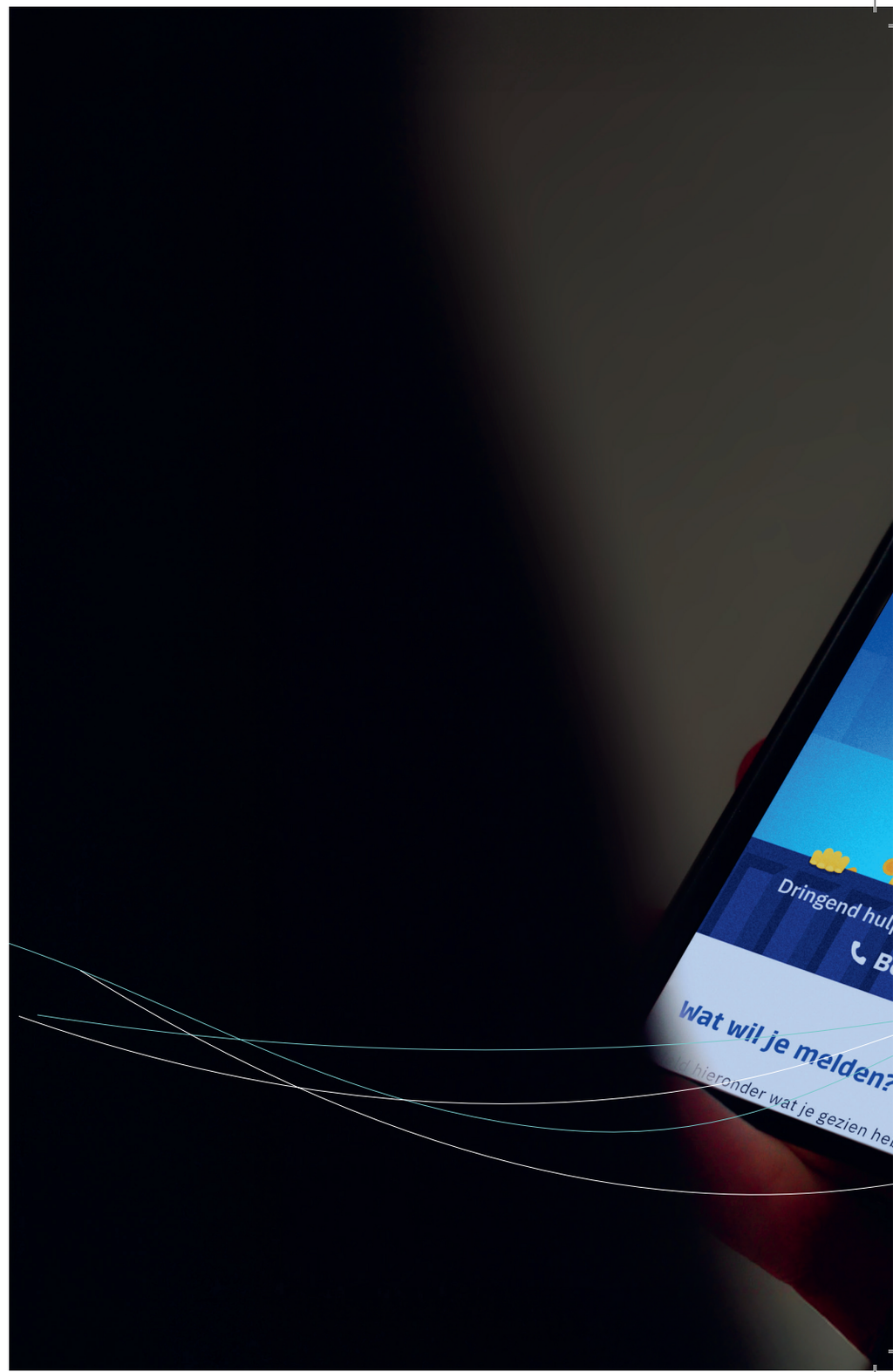
Les plateformes de signalement, les campagnes de sensibilisation et les formations ciblées constituent ensemble une approche intégrée en matière de sécurité et de sensibilisation. Nous veillons ainsi à détecter et à traiter rapidement les abus, la criminalité et les risques.

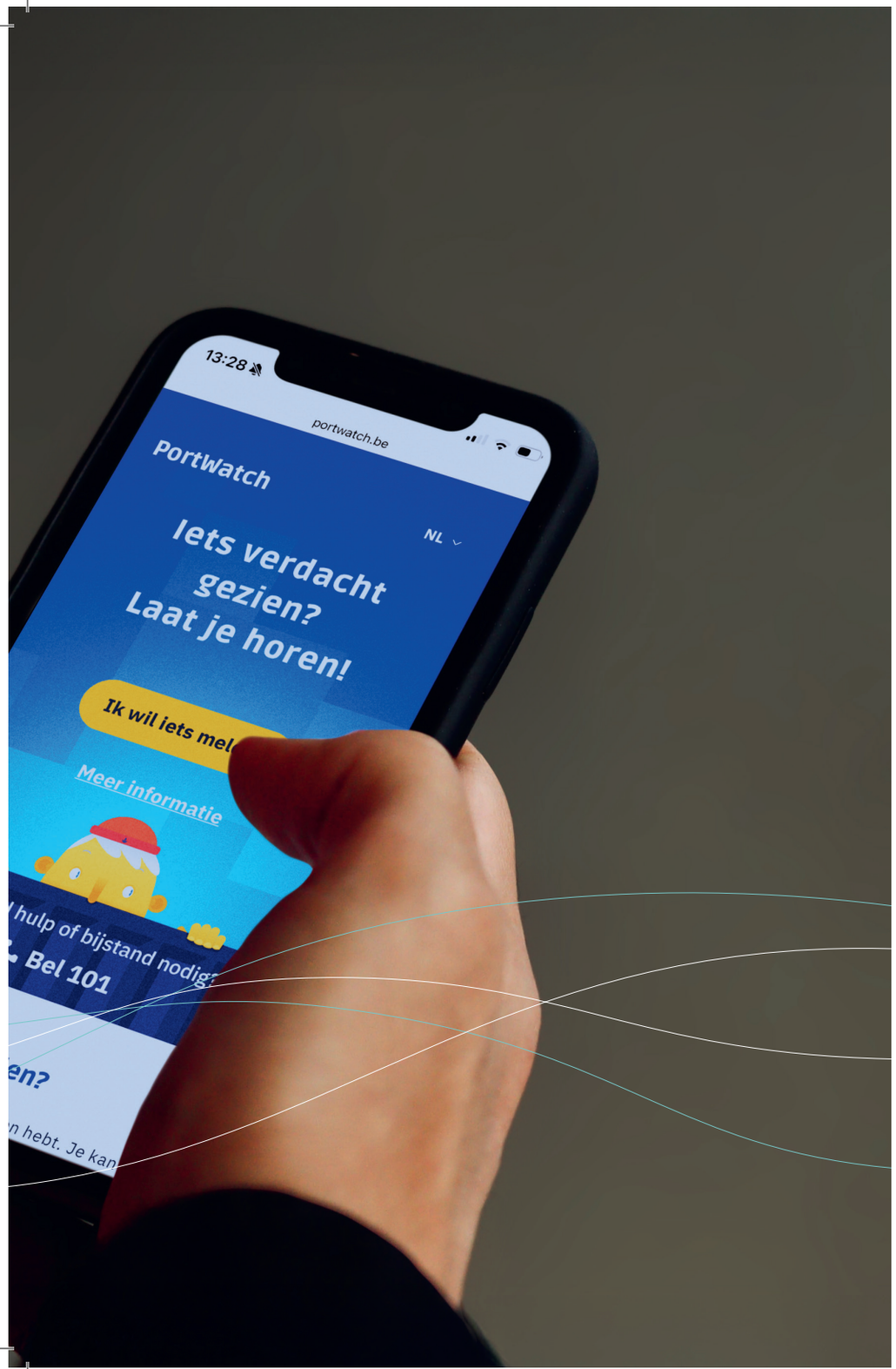
Une communauté portuaire résiliente

Les ports et installations portuaires belges investissent massivement dans la formation continue, les exercices conjoints et la sensibilisation ciblée. Ils souhaitent ainsi rendre leurs collaborateurs résistants aux influences criminelles et leur permettre de reconnaître à temps les risques. Tant le personnel opérationnel que les supérieurs hiérarchiques sont activement impliqués dans un réseau d'apprentissage en matière de sécurité. Il existe également plusieurs points de contact où les situations suspectes peuvent être immédiatement signalées à l'autorité compétente.

Découvrez Portwatch

Découvrez Notre port sans drogue





Les points de contact anonymes comme première ligne de défense

Portwatch
Portwatch est un point de contact anonyme et centralisé pour tous les ports et installations portuaires belges. Ce portail en ligne permet aux collaborateurs, aux visiteurs ou aux riverains de signaler facilement toute situation suspecte. Un système unique pour tout le pays.

Notre port sans drogue
À Port of Antwerp-Bruges, la plateforme « Onze Haven Drugsvrij » (Notre port sans drogue) constitue un point de contact supplémentaire spécifique à Anvers. Elle permet de signaler de manière anonyme tout comportement suspect lié à la criminalité liée à la drogue. Le point de contact est complémentaire à Portwatch : les deux points de contact se renforcent mutuellement et élargissent la portée de la prévention et de la détection.

Partenariat local de prévention Port
En outre, le Partenariat local de prévention (PLP) à Anvers assure une vigilance accrue entre les entreprises du port, la Police de navigation et Port of Antwerp-Bruges. Le réseau sensibilise les entreprises du port, notamment en partageant des conseils préventifs, mais les contacte également par téléphone en cas d'urgence.

Toutes les entreprises affiliées sont automatiquement reliées au système national BE-Alert. Ainsi, ils sont rapidement avertis en cas d'urgence dans le quartier.

Formations et sensibilisation

Manuel Exercitium
Les agents de sûreté portuaire (Port Facility Security Officers - PFSO) sont légalement tenus d'organiser des exercices et des formations au sein de leur installation. Pour les aider dans cette tâche, Port of Antwerp-Bruges a développé, à la demande de la Commission européenne, le manuel Exercitium. Il propose des scénarios et des idées préconçus pour réaliser des exercices de sécurité à petite et grande échelle dans les terminaux.

Exercices ISPS et Port Security
Depuis 2023, les agents de sûreté portuaire de North Sea Port organisent chaque année un exercice transfrontalier de sûreté portuaire à l'échelle du port. Les PFSO de Gand et de Terneuzen/Flessingue s'exercent simultanément selon le même scénario. Les installations ISPS auront également la possibilité d'organiser leur propre exercice annuel au même moment afin de partager efficacement leur expérience.

Découvrez le manuel Exercitium

Cours ISPS interne
Les services de sûreté portuaire d'Anvers et de Zeebruges ont développé leur propre cours de base ISPS qui explique les principales obligations du Code ISPS et de la loi sur la sûreté maritime. Cette formation est destinée au personnel qui travaille quotidiennement dans la zone portuaire ou dans des installations soumises au code ISPS, telles que les écluses et les terminaux de croisière.

Cours pour agents de surveillance
Pour les agents de surveillance affectés à des installations ISPS, la formation « Surveillance portuaire – EXE14 » est obligatoire. Ils y découvrent le port en tant qu'espace de travail, ce qu'est l'ISPS, comment les ports sont sécurisés et quelles sont les techniques de surveillance existantes.

Formation de sensibilisation pour les travailleurs portuaires
En outre, plusieurs prestataires de formation proposent des formations spécifiques en matière de sensibilisation à la sûreté. Ces formations courtes sensibilisent les collaborateurs aux risques, à leur responsabilité partagée et à la manière dont ils doivent agir correctement et en temps opportun.

Dans le Limbourg, le coordinateur d'entreprise de la ville de Genk a organisé une campagne de sensibilisation à l'intention de toutes les entreprises exerçant des activités liées à l'eau et situées dans la zone Genk-Sud. Le groupe de pilotage provincial a également élaboré en 2024 une campagne de sensibilisation à l'intention des entreprises et des installations portuaires de la zone Genk-Sud, axée principalement sur les entreprises exerçant des activités « à risque ».

Programme CPTED
La ville de Genk a mis en place un programme CPTED (Crime Prevention Through Environmental Design) dans la zone Logistics Valley Flanders. Ils ont également identifié les risques encourus par les nombreuses entreprises concernées.

Campagnes anti-recrutement
Grâce à des campagnes de sensibilisation, des simulations et des formations, notamment en collaboration avec des écoles supérieures et des entreprises de surveillance, les jeunes et les travailleurs apprennent à reconnaître et à repousser les approches suspectes.
North Sea Port a rendu obligatoire pour chaque membre du personnel une formation à la sensibilisation à la sûreté et une formation anti-recrutement. Cela s'inscrit dans le cadre de leur programme sur la résilience. En outre, North Sea Port met activement les formations anti-recrutement à la disposition des terminaux ISPS.

Les jeunes inscrits dans les hautes écoles qui suivent des filières liées au secteur logistique et portuaire bénéficient d'un programme spécifique intitulé « sensibilisation des jeunes », élaboré en collaboration avec le ministère public d'Anvers.

Campagne de sensibilisation pour le personnel portuaire et les marins
La DG Navigation et le Commissariat National Drogue travaillent à l'élaboration d'une approche nationale de la corruption dans les ports et chez les marins. Ils y parviennent grâce à des campagnes de sensibilisation et des outils sur mesure qui permettent au personnel d'être mieux armé grâce à ces informations et solutions.

Collaborer en matière de sûreté

« La collaboration est la clé. Personne ne peut mener ce combat seul. La police, la justice, les douanes, mais aussi les entreprises, les autorités portuaires et les syndicats doivent se concerter.
Les criminels opèrent au-delà des frontières et partagent rapidement les informations. Si nous ne le faisons pas, nous courons le risque d'être dépassés par les événements. »

Ine van Wymersch
Commissaire Nationale Drogue

Aucun port ne peut assurer sa sécurité dans l'isolement. C'est pourquoi le parquet, les douanes, les autorités portuaires et les entreprises privées collaborent de plus en plus étroitement dans les régions portuaires. Ils le font dans le cadre de structures de concertation communes ou de plateformes de sûreté multidisciplinaires. Tant dans les collaborations menées par un organisme public que dans les collaborations public-privé. Celles-ci permettent un échange d'informations plus rapide, une approche commune de la criminalité organisée et le déploiement d'applications de sûreté innovantes.

Réseaux locaux

Collaborations public-privé au niveau local

Data Community in North Sea Port

La Data Community au sein du North Sea Port est un excellent exemple de collaboration public-privé. Ce réseau rassemble les entreprises du port et l'autorité portuaire elle-même autour d'une mission commune : renforcer l'écosystème numérique dans la chaîne nautique et logistique, avec la sûreté comme thème central.

La Data Community s'articule autour de deux piliers stratégiques :

1. **Une collaboration numérique intelligente au sein de la chaîne**
   Grâce à un meilleur échange de données, les arrivées, les départs et les flux logistiques gagnent en efficacité et en transparence.
2. **Approche collective du contrôle d'identité et d'accès**
   Les entreprises harmonisent leurs procédures d'accès afin d'établir une norme d'accès uniforme et fiable dans toute la région portuaire.

Ces ambitions sont traduites du stade pilote à la pratique via le North Sea Portal, le nœud numérique central pour l'échange sécurisé de données. La première réalisation concrète est l'introduction du Port Pass : une clé d'accès numérique commune avec identification biométrique, déployée dans plusieurs grandes entreprises de la zone portuaire de Gand.

Security Think Tank
Le Security Think Tank est un partenariat public-privé qui représente divers utilisateurs portuaires, prestataires de services et autorités. Il se réunit trois fois par an pour discuter de divers sujets liés à l'ISPS et à la sûreté portuaire.

Partenariat public-privé Genk
Actuellement, la ville de Genk travaille à la mise en place d'un partenariat public-privé sous la forme d'une chaîne de confiance, dans le cadre de laquelle les entreprises sont régulièrement sensibilisées.

Agents de sûreté portuaire
North Sea Port organise tous les deux ans des sessions d'information ISPS pour les PFSO des deux régions du pays. Par ailleurs, des sessions ad hoc sont organisées à Gand autour de thèmes spécifiques, avec la participation des PFSO et des PDG des terminaux ISPS. Port of Antwerp-Bruges organise des sessions similaires pour les PFSO, au cours desquelles des informations importantes sont partagées et où les participants ont également la possibilité de nouer des contacts entre eux. En outre, des thèmes tels que les risques et les menaces, les mesures et les bonnes pratiques ainsi que la nouvelle législation y sont abordés. Des conférenciers sont régulièrement invités.

Taskforce Containers
La Taskforce Containers est une nouvelle initiative lancée à Anvers afin de partager, dans un cadre confidentiel, les meilleures pratiques, les mesures et les points faibles en matière de sûreté entre différents terminaux.

Collaborations publiques au niveau local

Groupe de pilotage « Zone avec notification globale » (ZNG)
La Défense organise régulièrement des exercices dans le Port of Antwerp-Bruges comme moyen de dissuasion supplémentaire. Cela est inscrit dans un protocole spécifique dans lequel les membres du groupe de pilotage ZNG sont informés des exercices et peuvent imposer des conditions supplémentaires.

Tableau stratégique Stroomplan 2.0
Il s'agit du plan local de lutte contre la drogue à Anvers, sous la direction du procureur du Roi. Le plan prévoit diverses mesures s'articulant autour de quatre axes : barrières dans le port, approche intégrée, amélioration de la recherche et politique d'intégrité. Des initiatives similaires ont été lancées dans le Limbourg et à Gand.

Comité local pour la sûreté maritime
Le Comité local pour la sûreté maritime (CLSM) est l'autorité locale compétente pour l'ISPS dans chaque port ou voie navigable doté d'installations portuaires. Le comité se réunit quatre fois par an, ou de manière ad hoc si nécessaire. Ici aussi, la composition et le fonctionnement sont imposés par la loi.

Le Limbourg occupe une position unique à cet égard : il ne dispose pas de port, mais on y trouve plusieurs installations portuaires. C'est pourquoi il n'y a pas de service de capitainerie portuaire à part entière. Ils compensent cela par leur action CLSM et en misant sur un partenariat solide avec les différents acteurs de la sécurité.

Comité de pilotage provincial Limbourg
Le gouverneur du Limbourg a pris l'initiative de créer un groupe de pilotage provincial afin d'identifier et d'échanger les meilleures pratiques entre les différentes installations portuaires.

Réseaux nationaux

Autorité nationale de sécurité maritime
L'Autorité nationale de sécurité maritime (ANSM) est l'autorité nationale compétente pour l'ISPS. Elle se réunit quatre fois par an, ou ponctuellement si nécessaire. Sa composition et son fonctionnement sont imposés par la loi.

Réseaux européens et internationaux

Port Security Steering Committee
Le Port Security Steering Committee est une collaboration entre les trois plus grands ports d'Europe : Rotterdam, Anvers-Bruges et Hambourg. Ils collaborent dans le cadre de trois groupes de travail : normes ISPS et mesures innovantes, modus operandi et coopération avec l'Amérique du Sud. Une lettre d'intention a également été signée avec d'autres ports de la ligne Hambourg-Le Havre afin de les tenir informés des développements au sein des groupes de pilotage et de travail.

Partenariat public-privé de l'alliance des ports européens (EPA PPP)
Afin de lutter contre l'infiltration croissante des réseaux criminels dans les ports européens, la Commission européenne a lancé l'EPA PPP le 24 janvier 2024, sous la présidence belge de l'UE. Ce partenariat public-privé rassemble toutes les parties prenantes dans une approche commune contre le trafic de drogue et le crime organisé.

Pan-Atlantic Cooperation
La Pan Atlantic Cooperation est une coopération entre les autorités ISPS compétentes des trois plus grands ports de l'UE et de la Colombie, de l'Équateur et du Pérou. Ils utilisent l'ISPS comme lien pour partager et améliorer les bonnes pratiques en matière de prévention et de sûreté portuaire.

Périmètre et accès

« La sûreté maritime de nos installations portuaires contribue à relier les régions, à renforcer l'économie et à favoriser le développement durable. Un contrôle d'accès et un enregistrement stricts, par exemple via ItsMe®, sont essentiels pour garantir l'intégrité de notre chaîne logistique. Nous renforçons ainsi la sécurité et l'efficacité de nos installations portuaires. »

Robin Minten
Président du CLSM Limbourg et
directeur-coordinateur de la Police fédérale du Limbourg

Une sûreté solide commence à l'entrée. Les ports et installations portuaires belges investissent donc dans des solutions modernes d'accès et de périmètre qui sont à la fois adéquates et conviviales.

Les plateformes numériques, les moyens d'identification intelligents et les infrastructures innovantes garantissent que seules les personnes autorisées peuvent accéder aux zones appropriées et que chaque accès reste traçable et contrôlable.

Systèmes de contrôle d'accès numériques

Alfapass
Alfapass est un système d'identification et d'autorisation numérique dans le port d'Anvers-Bruges. Grâce à un badge centralisé, les travailleurs, les visiteurs et les prestataires de services peuvent s'identifier aux terminaux et aux installations. L'initiative est née des besoins du secteur privé. Divers acteurs utilisent désormais ce système grâce à sa facilité d'intégration dans les processus opérationnels et les systèmes de portails.

Prean
Prean est une plateforme en libre-service permettant aux visiteurs de s'enregistrer à l'avance lorsqu'ils se rendent sur des navires ou dans des zones portuaires. Bien que Prean n'accorde pas lui-même l'accès, il centralise toutes les informations nécessaires pour décider si une personne peut accéder à un endroit et simplifie la gestion des visiteurs pour les entreprises, les agences et les installations portuaires.

Peripass
North Sea Port développe également une solution uniforme via Peripass, une plateforme de gestion de chantier naval et d'accès qui est déployée en collaboration avec les installations ISPS en tant que Port Pass central. Cette solution combine la planification, le contrôle d'accès et le flux logistique dans un seul système et constitue le premier résultat concret de leur communauté de données.

ItsMe®
Les installations portuaires limbourgeoises Port of Limburg démontrent que les ports intérieurs sont également à la pointe en matière de sécurité technologique. En tant que port intérieur parmi les plus sécurisés du Benelux, elles ont collaboré avec SCR et ItsMe® pour mettre en place un processus d'identification numérique répondant aux normes les plus strictes.

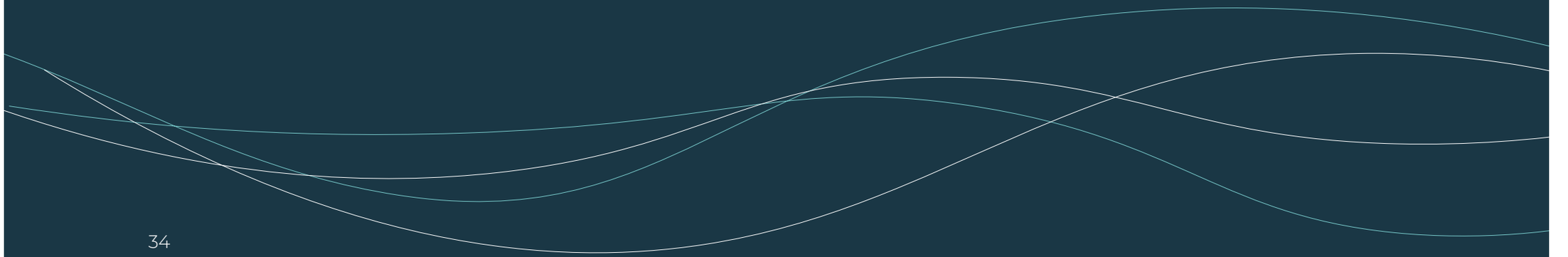
Clôture intelligente

Outre les solutions numériques, la sécurité physique devient également plus intelligente. Une clôture intelligente est déployée dans Port of Antwerp-Bruges. Cette infrastructure est équipée de capteurs de détection et, associée à une technologie de caméras et à une surveillance en temps réel, elle offre une protection maximale contre les tentatives d'intrusion.

North Sea Port mise également sur des clôtures intelligentes, avec la construction de trois kilomètres de clôtures comme ligne de défense supplémentaire contre la criminalité.

Port of Limburg dispose également de capteurs de détection et de caméras thermiques qui couvrent l'ensemble du périmètre/de la clôture. Ils signalent immédiatement toute intrusion au téléphone portable des responsables. Ils peuvent visionner directement les images des caméras sur leur téléphone portable.

Détection



« La détection est importante pour garantir la sécurité et le bon fonctionnement d'un port. Grâce à la salle de contrôle centrale située à Zeebruges, nous rassemblons les données de nombreux services de sécurité afin d'améliorer l'efficacité de la surveillance et de la collaboration. Nos caméras intelligentes y contribuent également en détectant les risques et en alertant immédiatement la salle de contrôle centrale. Nous renforçons ainsi la sécurité des personnes, des infrastructures et de la navigation. »

Kim Pettens
Président LCMB Zeebrugge et
capitaine du port de Zeebruges à Port of Antwerp-Bruges

Un port moderne n'est pas seulement une plaque tournante logistique, mais aussi une zone spécifique hautement sécurisée où tout risque doit être détecté à un stade précoce. C'est pourquoi les ports belges investissent dans un vaste réseau de détection combinant terre, mer et air. D'un réseau radar sophistiqué à des caméras intelligentes et des drones : la technologie fait office d'yeux et d'oreilles de la zone portuaire.

Surveillance centralisée depuis les salles de contrôle

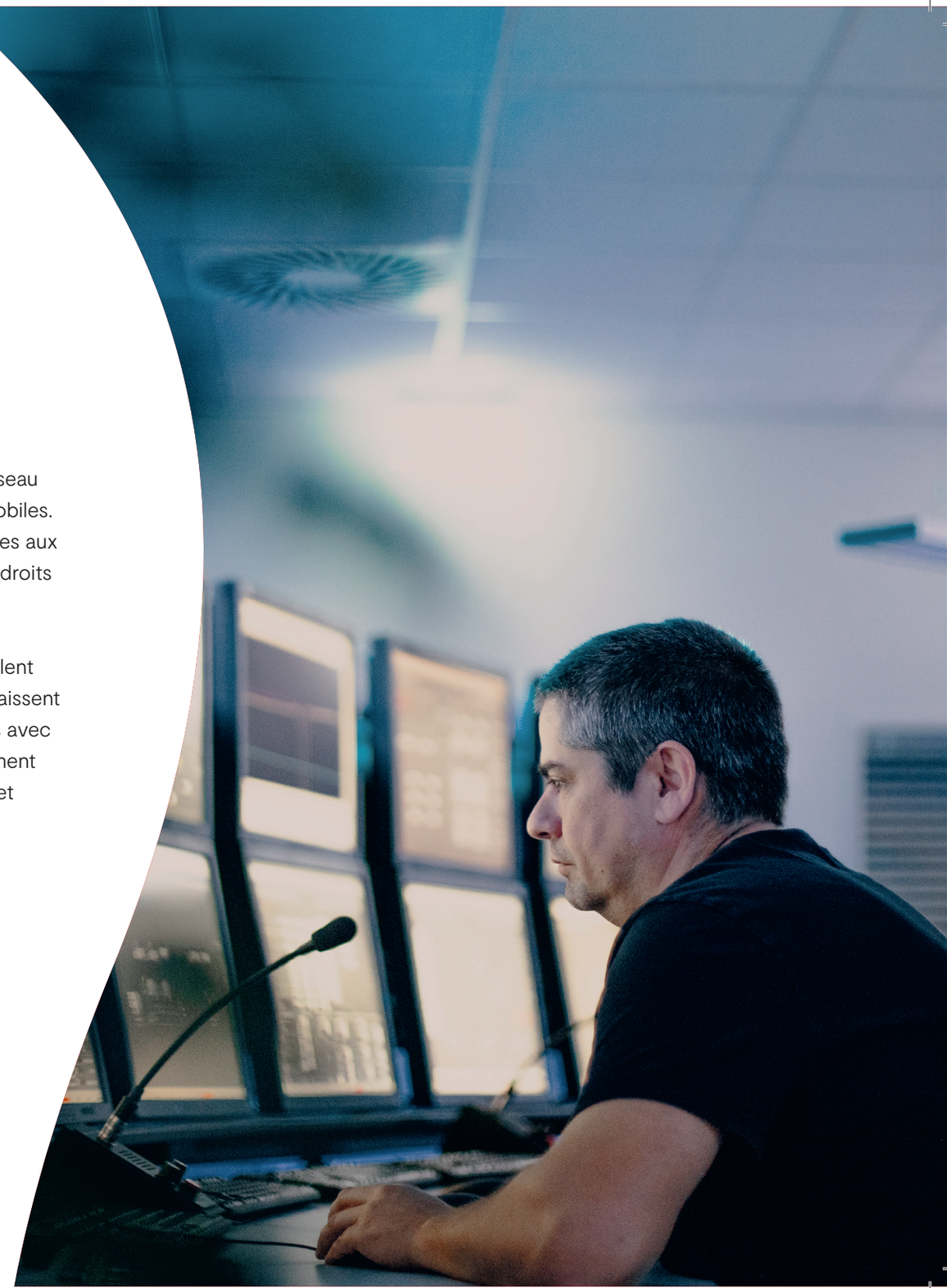
Vessel Traffic Center
Le Vessel Traffic Center constitue la colonne vertébrale de la surveillance maritime. Il s'agit d'une salle de contrôle centralisée qui surveille le trafic maritime. Grâce à un vaste réseau de radars et de caméras, le Vessel Traffic Services (VTS) surveille en permanence le trafic maritime dans et autour des zones portuaires. À Anvers, cela se fait depuis l'Antwerp coordination center (ACC).

Central Control Room
La Central Control Room (CCR) a été installée à Zeebruges. Elle améliore la communication, la sûreté et la sécurité des activités portuaires. Des centaines de caméras appartenant à des services de sécurité d'entreprises privées sont reliées à la salle de contrôle, où toutes ces images sont surveillées.

Réseaux de caméras basés sur l’IA

Les terminaux d’Anvers et le North Sea Port disposent d’un vaste réseau de caméras ANPR (Automatic Number Plate Recognition) fixes et mobiles. Ces systèmes enregistrent les plaques d’immatriculation des véhicules aux portes, routes et terminaux et les associent automatiquement à des droits d’accès ou à des profils de risque.

Des caméras intelligentes dotées d’une intelligence artificielle surveillent également les ports d’Anvers et de Zeebruges. Ces caméras reconnaissent les navires, facilitent le suivi des incidents et peuvent être partagées avec les services de sécurité. Les caméras intelligentes détectent rapidement et facilement les personnes et les problèmes dans le réseau routier et alertent immédiatement la salle de contrôle centrale.



Drones

L'espace aérien prend une importance croissante dans le domaine de la détection. À Anvers, un réseau permanent de drones est opérationnel pour soutenir les inspections, les observations et les interventions d'urgence depuis les airs. North Sea Port utilise également des drones pour ses inspections et développe actuellement un système supplémentaire de détection des drones afin d'intercepter à temps les appareils indésirables. Il y a aussi un « drone in the box » sur le toit du Port of Limburg. La police locale l'utilise en cas d'incidents dans la zone Genk-Sud, où se trouvent la plupart des installations portuaires du Limbourg.

À Zeebruges, une plateforme de détection des drones permet à la salle de contrôle centrale de surveiller l'espace aérien 24 heures sur 24, 7 jours sur 7. Ils tiennent compte des menaces externes telles que l'activisme climatique, la présence de navires militaires de l'OTAN ou non, etc.

Scanners mobiles

Enfin, les scanners mobiles pour conteneurs utilisés par les douanes complètent l'arsenal de détection. Cet équipement permet de contrôler rapidement, localement et de manière ciblée les marchandises sans entraîner de retard logistique important. Ils évitent le transfert du conteneur, sous escorte, vers un poste d'inspection frontalier, ce qui rend la procédure de scan plus efficace et plus rapide.

Navires de patrouille

Sur l'eau, tant la Police de navigation que les autorités portuaires assurent une présence visible grâce à des navires de patrouille modernes. La Police de navigation a récemment mis en service de nouveaux navires qu'elle utilise aussi bien dans les ports que sur les voies navigables menant aux ports.

Ainsi, la Police de navigation de Gand dispose d'un navire de patrouille pour la zone portuaire et d'un navire d'intervention rapide. Port of Antwerp-Bruges a également mis en service deux patrouilleurs en 2022. Dans le port d'Anvers, la Police de navigation peut déployer deux patrouilleurs et un navire d'intervention rapide. Avec la création d'un poste de la Police de navigation dans le Limbourg en 2023, un nouveau patrouilleur a également été mis en service en 2024.

Sûreté portuaire

En raison de l'importance nationale du port d'Anvers, la Police de navigation déploie, outre les équipes d'intervention habituelles, une équipe spécifique chargée de la sûreté portuaire. Celle-ci assure la sécurité du port en tant qu'infrastructure vitale contre les organisations terroristes et criminelles.

Autres projets de sûreté

En plus de la surveillance physique et du contrôle d'accès, les ports belges investissent également dans des systèmes innovants qui renforcent la sécurité à chaque maillon de la chaîne logistique, tant au niveau du terminal lui-même que dans l'environnement numérique.

Certified Pick-Up : contrôle jusqu'à la porte du conteneur

Avec Certified Pick-Up, Port of Antwerp-Bruges a introduit un mécanisme de libération entièrement numérique et sécurisé pour les conteneurs. Là où l'on utilisait auparavant des documents papier ou des codes PIN, le système fonctionne désormais via une chaîne d'autorisation intégrée et liée à l'identité. Seul le transporteur correctement enregistré aura accès au conteneur au moment de l'enlèvement.

Résultat : moins de fraudes, moins d'abus de codes PIN et une traçabilité totale de chaque transfert. Au bout d'un an, plus d'un million de conteneurs avaient déjà été libérés via ce système, ce qui témoigne clairement de sa large acceptation au sein du secteur.

Port of Limburg assure également la sécurité du processus de retrait des conteneurs grâce au système Secured Container Release de T-Mining, couplé à ItsMe®.

Digital Twins : la vision virtuelle de la réalité

Afin de réagir plus rapidement et plus efficacement aux incidents, les ports développent des plateformes Digital Twins (telles que APICA chez Port of Antwerp-Bruges). Ces copies numériques de la zone portuaire combinent des données en temps réel provenant de capteurs, de caméras, de systèmes de circulation et d'informations météorologiques.

Les opérateurs disposent ainsi d'un « troisième œil » sur le terrain, qui leur permet de surveiller et de simuler plus efficacement les opérations quotidiennes et les situations d'urgence. Les Digital Twins deviennent ainsi des outils stratégiques pour la détection des incidents, la planification et l'analyse des risques.

Cyber-résilience

La résilience numérique est tout aussi essentielle que la sécurité physique. C'est pourquoi plusieurs ports déploient actuellement des programmes de cyber-résilience.

Port of Antwerp-Bruges dispose d'une cyber-équipe spécialisée qui travaille selon le modèle des trois lignes de défense : surveillance opérationnelle, expertise et conseil, et audits internes. Le contrôle actif des identités, la gestion automatisée des accès et la surveillance des actifs via des plateformes telles qu'Armis permettent de détecter immédiatement les appareils ou connexions non autorisés. La prévention reste toutefois cruciale : grâce à des programmes de sensibilisation, tous les collaborateurs de l'autorité portuaire d'Anvers-Bruges sont préparés à d'éventuels incidents.

North Sea Port collabore avec d'autres ports maritimes néerlandais à la mise en place d'une plateforme nationale de cybersécurité, sous la coordination des pouvoirs publics et des services de sécurité. Le partage des connaissances, l'analyse conjointe des menaces et la formation permettent de renforcer la résilience des entreprises de la chaîne portuaire.

Des initiatives telles que la session d'inspiration « Cyber Resilience in de Haven » (Cyber-résilience dans le port) d'Alfaport Voka montrent comment la sensibilisation et la coopération sont essentielles pour rendre la ligne de défense numérique aussi solide que la ligne de défense physique.

Port 2 Port

Plate-forme de sécurité