

Port 2 Port

Security Platform





Inhoud

Samen sterk	4
Wetgeving & inspecties	8
Meldpunten en opleidingen	16
Samenwerken rond beveiliging	22
Perimeter en toegang	28
Detectie	34
Andere beveiligingsprojecten	40

Samen sterk

De Belgische havens zijn poorten naar de wereld. Ze verbinden mensen, goederen en industrie, maar waar die stromen samenkomen, schuilen ook risico's. Georganiseerde criminaliteit en grensoverschrijdende dreigingen vragen vandaag meer dan ooit om een gezamenlijke, geïntegreerde aanpak. Vanuit verschillende havens groeide dan ook de vraag om op vlak van beveiliging best practices te bundelen en structureel samen te werken. Die gedeelde ambitie vormde de basis voor het Port 2 Port Security Platform.

Port 2 Port Security Platform is een gezamenlijk initiatief van Port of Antwerp-Bruges, North Sea Port en Federale Politie CSD Limburg, in nauwe samenwerking met het Nationaal Drugscommissariaat. Het platform, dat op 21 november 2025 gelanceerd werd, verenigt alle Belgische zee- en binnenhavens. Een nieuwe stap om onze havens weerbaarder te maken in een continu veranderende maatschappij.

Samen sterk

**Onze havens:
open voor wereldhandel,
gesloten voor criminaliteit.**



Samen sterk

Met de aanstelling van Ine Van Wymersch als eerste Nationale Drugscommissaris kreeg België één aanspreekpunt in de strijd tegen georganiseerde misdaad en druggerelateerde criminaliteit. Vanuit haar rol bouwt ze samen met haar collega's van het Nationaal Drugscommissariaat aan een geïntegreerde, nationale strategie die politie, justitie, havens, bedrijven en burgers verenigt rond één doel: onze samenleving en economische poorten weerbaar maken tegen criminele infiltratie. Die aanpak kreeg vorm in de IJsbergstrategie.



Samenwerking is geen optie, maar een noodzaak

“Onze havens zijn economische motoren van wereldformaat,” zegt Ine Van Wymersch. “Elke dag passeren er duizenden mensen, goederen en schepen. Die enorme dynamiek is een sterkte, maar tegelijk ook een kwetsbaarheid. Criminele organisaties proberen binnen te dringen in die logistieke keten – vaak subtiel, via technologie of de goedgelovige zwakste schakels.”

Volgens Van Wymersch is samenwerking de sleutel. “Niemand kan deze strijd alleen voeren. Politie, justitie, douane, maar ook bedrijven, havenautoriteiten en vakbonden moeten elkaar vinden. Criminelen werken grensoverschrijdend en delen informatie snel. Als wij dat niet doen, lopen we achter de feiten aan.”

Ze benadrukt dat goede praktijken en inzichten niet mogen blijven hangen binnen één haven. “Wat vandaag werkt in Antwerpen of Gent, kan morgen het verschil maken in Luik of Brussel. We moeten onze kennis delen, anders verliezen we kostbare tijd. Havenautoriteiten spelen daarbij een cruciale rol: zij verbinden de publieke en private wereld.”

De IJsbergstrategie: inhakken op de ijsberg en de temperatuur van het water opwarmen

Van Wymersch gebruikt graag de metafoor van een ijsberg om de nationale aanpak te beschrijven. “De criminele organisaties zijn de ijsberg. Wat we zien zijn de drugsvangsten, schietpartijen en ontploffingen. Maar dat is slechts het topje van de ijsberg,” legt ze uit. “Onder de waterlijn speelt het veel grotere, onzichtbare deel: witwaspraktijken, corruptie, chantage, misbruik van werknemers. Als we alleen rechtstreeks inhakken op de ijsberg, vanuit de repressieve overheid, maar niet inzetten op de temperatuur van het water, door de weerbaarheid te verhogen van organisaties en werknemers, blijft het koud in ons ecosysteem. En waar het koud is, smelt de criminele ijsberg niet.”

Daarom koppelt de IJsbergstrategie twee aanpakken aan elkaar. “Enerzijds hebben we de directe aanpak: politie, justitie en douane die kordaat ingrijpen (of het ijs weggappen). Anderzijds investeren we in de indirecte aanpak: preventie, opleiding, bewustmaking, weerbaarheid. Wie zijn mensen traint, HR-beleid versterkt en informatie-uitwisseling organiseert, warmt het water op. Zo smelt de ijsberg en wordt ook de directe aanpak veel effectiever.”

Eén ecosysteem, één verantwoordelijkheid

Voor Van Wymersch is duidelijk dat beveiliging niet ophoudt aan de poort van de haven.

“Rederijen, terminals, logistieke bedrijven, vakbonden, overheden en internationale partners – ze maken allemaal deel uit van hetzelfde ecosysteem. Als één partij buiten dat netwerk blijft, ontstaat er ruimte voor criminaliteit. Alleen door samenwerking en open communicatie kunnen we die ruimte dichten.”

Ze roept alle betrokkenen op om niet te wachten op anderen. “De toekomst vraagt actie, geen afwachten. Iedere havenautoriteit kan het verschil maken door informatie te delen, risico's te benoemen en de ijsbergstrategie als gemeenschappelijk kompas te gebruiken. Zo maken we van onze havens niet enkel economische knooppunten, maar ook plekken waar eerlijke concurrentie, handhaving en weerbaarheid hand in hand gaan.”

Wetgeving & inspecties

“De herziene Wet Maritieme Beveiliging tilt de beveiligingsstandaard in onze haven naar een nieuw niveau. Dankzij deze wet kunnen we risico's sneller detecteren en doeltreffender optreden tegen criminele activiteiten. Ze laat ons toe om de veiligheid van mensen, goederen en infrastructuur structureel te versterken. Dat is essentieel voor een betrouwbare en toekomstgerichte haven.”



Niels Vanlaer

Voorzitter LCMB Antwerpen en
havenkapitein bij Port of Antwerp-Bruges

Havenbeveiliging is geen lappendeken van losse maatregelen, maar bouwt op een stevig internationaal kader in de vorm van de ISPS-code, aangevuld met nationale wetgeving en lokale initiatieven. België behoort daarbij tot de voorlopers in Europa met de Wet Maritieme Beveiliging.

ISPS: Een gedeelde beveiligingsstandaard

De basis voor maritieme beveiliging ligt vast in de International Ship & Port Facility Security Code (ISPS). Deze wereldwijde norm is verplicht voor internationaal varende passagiersschepen, vrachtschepen met een bruto tonnage van 500 ton of meer, mobiele offshore boorplatforms en havenfaciliteiten die deze schepen ontvangen.

Om beveiligingsrisico's te identificeren en doeltreffende maatregelen te nemen zijn Port Facility Security Assessments en Port Facility Security Plans wettelijk verplicht. Deze omvatten onder meer procedures rond toegangscontrole, bewaking, toezicht op lading en richtlijnen voor incidenten en oefeningen.

De ISPS-code voorziet naast het installeren van beveiligingsinfrastructuur en -procedures ook een kader voor (inter)nationale samenwerkingen tussen publieke en private actoren in de maritieme sector.

België toont ambitie met Wet Maritieme Beveiliging

De beveiligingsmaatregelen uit ISPS zijn overgenomen in de Europese Verordening (725/2004). België zette deze internationale bepalingen om in nationale wetgeving via de Wet Maritieme Beveiliging, opgenomen in het Belgisch Scheepvaartwetboek. Die wet gebruikt het framework van de ISPS-code om georganiseerde criminaliteit aan te pakken waarbij het kader, de structuur en de mogelijkheden die overheid en bedrijven hebben, werden uitgebreid.

Ondertussen onderging de wet al twee herzieningen, die de beveiligingsstandaard nog hoger leggen. Op die manier maakt de wet meer mogelijk op vlak van beveiliging in de havens. Ze versterkt de beveiliging van havens en havenfaciliteiten en legt de nadruk op preventie van illegale activiteiten zoals drugsmokkel en mensenhandel. Tegelijk beschermt ze vitale infrastructuur, personeel en installaties tegen ongeoorloofde acties.



De Belgische wetgeving introduceert een reeks vernieuwende maatregelen die bijdragen aan een moderne, geïntegreerde beveiligingsaanpak:



Bijzonder uittreksel uit het strafregister: met dit nieuwe document controleren werkgevers de strafrechtelijke achtergrond van personen die in de haven of bij havenfaciliteiten willen werken.



Havenverboden via het AIGIS-platform: via het AIGIS-platform voorziet de wet in de mogelijkheid van controle op een havenverbod. Dat is een strafmaatregel voor het overtreden van de drugswetgeving en andere criminele feiten.



Veiligheidsverificaties via het PANOPTES-platform: het PANOPTES-platform maakt de verplichte veiligheidsverificatie mogelijk van personen met kritieke functies in de haven of havenfaciliteiten, zoals personen met toegang tot bepaalde bedrijven, goederen, IT-systemen, personeelsbeleid, haveninformatie...



Gebruik van biometrie en slimme camera's: een uitbreiding van het wettelijk kader voor geavanceerde toegangscontrole en cameratoezicht in de haven, havenfaciliteiten en op het Belgische deel van de Noordzee.



Risicogebaseerde beveiliging: binnenvaartterminals en bedrijven met een impact op de maritieme beveiliging kunnen op basis van een risicoanalyse ook onderworpen worden aan een set van minimumeisen rond beveiliging.



Ontdek het
AIGIS-platform

Bevoegde ISPS autoriteiten

De herziene Wet Maritieme Beveiliging zorgt voor een structurele en geautomatiseerde aanpak van de beveiliging in de Belgische havens en havenfaciliteiten. De wet verbetert de samenwerking en informatie-uitwisseling tussen de verschillende instanties zoals de Lokale Politie, DG Scheepvaart, Scheepvaartpolitie, Douane, Defensie, Nationaal Crisiscentrum, Veiligheid van de Staat, Algemene Dienst Inlichtingen en Veiligheid, Coördinatieorgaan voor de dreigingsanalyse, de havens (Port Security Officers), Cel Maritieme Beveiliging, Provinciaal Commando en de Gewesten.

De Nationale Autoriteit Maritieme Beveiliging (NAMB), onder het voorzitterschap van de FOD Mobiliteit en Vervoer, zorgt voor de implementatie en uitwerking van de wet. Voor de dagelijkse opvolging wordt de NAMB ondersteund door de Cel Maritieme Beveiliging (CMB).

In elke haven of waterweg met havenactiviteit is er een Lokaal Comité Maritieme Beveiliging (LCMB). In totaal zijn er in België negen LCMB's aanwezig. Die coördineren samen met de CMB de praktische implementatie van ISPS in hun havengebied. Zo'n LCMB is een krachtig en uniek platform waar de belangrijkste beveiligingspartners uit het havengebied samenkomen. Dankzij het lokale karakter zitten er vooral mensen aan tafel die het gebied door en door kennen. Doordat alle deelnemers beschikken over een veiligheidsmachtiging, kan gevoelige informatie op een veilige en vertrouwelijke manier gedeeld worden.

Kennisdeling als hefboom voor kwaliteit

Port of Antwerp-Bruges, Rotterdam en Hamburg ontwikkelden samen een gezamenlijke norm om de ISPS perimeter- en toegangscontroles te verbeteren. Die stelt autoriteiten en havenexploitanten in staat om beveiligingsmaatregelen te bepalen op basis van een afgesproken risicostandaard. Die standaard is in België ondertussen ook al verplicht gemaakt.



Lokale initiatieven

Naast internationale standaarden spelen lokale initiatieven een belangrijke rol in de versterking van de ISPS-beveiliging. Zo kunnen havens ook individueel een stapje verder gaan. Via de havenpolitieverordening maken Port of Antwerp-Bruges en North Sea Port de toegangscontrolemaatregelen verplicht voor álle bedrijven in het havengebied. Hierdoor blijft beveiliging niet langer beperkt tot strikt ISPS-plichtige sites.

In Limburg werkt de provinciale stuurgroep samen met de stad Genk een gelijkaardige politieverordening uit.

In North Sea Port (Gent) voeren havenluitnants bovendien tussentijdse ISPS-inspecties uit op basis van een eigen, lokale checklist. Daarvoor gebruiken ze een zelfontwikkelde toepassing, die een gestructureerde planning en monitoring mogelijk maken. Bij Port of Antwerp-Bruges staat een team van Port Authority Officers klaar om dagelijks een oogje mee in het zeil te houden en tekortkomingen in beveiliging te rapporteren aan het LCMB.



Ontdek de
ISPS-havenbeveiligingsnormen
in deze brochure

Websites rond beveiliging

Voor meer informatie kan je terecht op de ISPS en Port Security websites van de Belgische Havens:



**Port of
Antwerp-Bruges**



North Sea Port



DG Scheepvaart



Meldpunten en opleidingen

Bewustwording is onze eerste verdedigingslijn tegen criminaliteit. Het is belangrijk dat we die alertheid bij iedereen in of rond de haven aanwakkeren. Zo leren we met ronselproof-trainingen onze medewerkers en jongeren hoe ze ronselpogingen herkennen en afwijzen. Meldpunten als Portwatch maken het eenvoudig om verdachte situaties anoniem te melden. Zo versterken we samen de weerbaarheid en integriteit van onze haven.”



Wim Van Bogaert

Voorzitter LCMB Gent en
havenkapitein bij North Sea Port

Medlpunten en opleidingen

Meldplatformen, sensibiliseringscampagnes en gerichte opleidingen vormen samen een geïntegreerde beveiligings- en bewustwordingsaanpak. Zo zorgen we ervoor dat we misbruik, criminaliteit en risico's vroegtijdig detecteren én aanpakken.

Een weerbare havengemeenschap

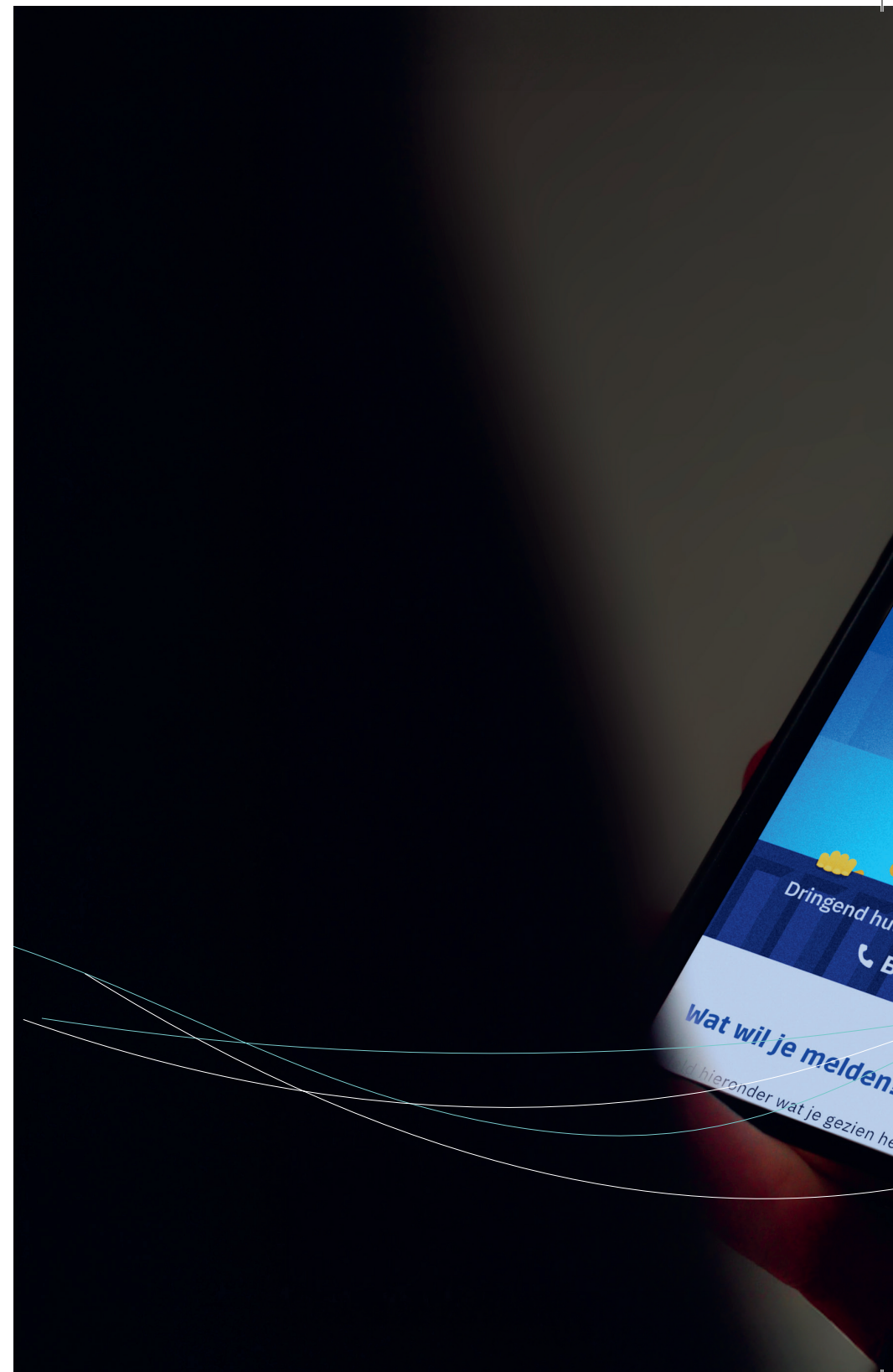
Belgische havens en havenfaciliteiten investeren fors in permanente opleiding, gezamenlijke oefeningen en gerichte sensibilisering. Zo willen ze medewerkers weerbaar maken tegen criminele invloeden en in staat stellen om risico's op tijd te identificeren. Zowel operationeel personeel als leidinggevenden worden actief betrokken in een lerend beveiligingsnetwerk. Daarnaast zijn er ook verschillende meldpunten waar verdachte situaties meteen bij de juiste instantie gemeld kunnen worden.



Ontdek
Portwatch



Ontdek Onze
Haven Drugsvrij



Anonieme meldpunten als eerste verdedigingslinie

Portwatch

Portwatch is een anoniem, centraal meldpunt voor alle Belgische havens en havenfaciliteiten. Via dit online portaal kunnen medewerkers, bezoekers of omwonenden verdachte situaties eenvoudig rapporteren. Een uniek systeem voor het hele land.

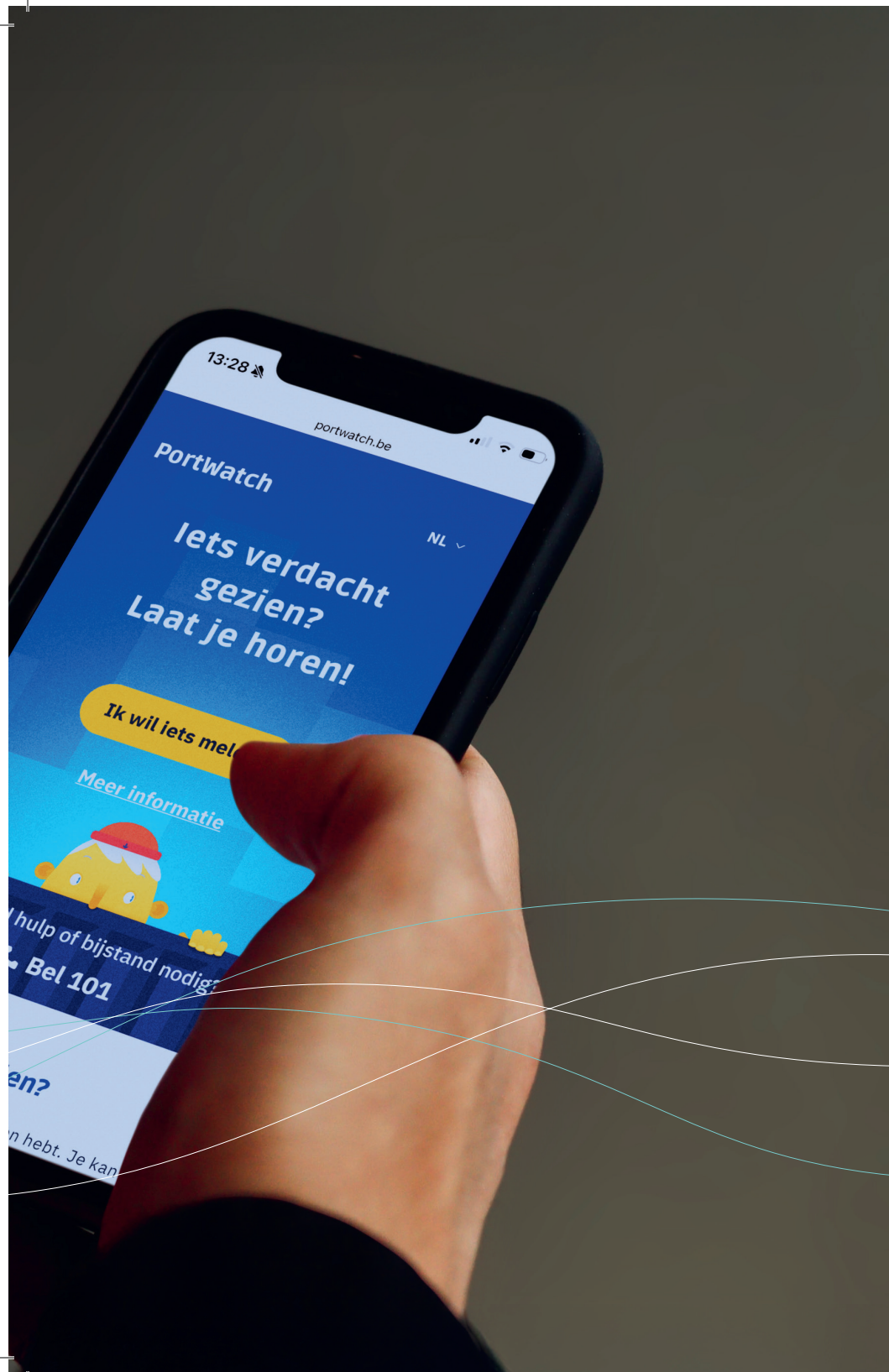
Onze Haven Drugsvrij

In Port of Antwerp-Bruges vormt het platform Onze Haven Drugsvrij een bijkomend meldpunt voor Antwerpen specifiek. Hier kan je anonieme meldingen maken van verdacht gedrag in het kader van drugscriminaliteit. Het meldpunt is complementair aan Portwatch: beide meldpunten versterken elkaar en vergroten de reikwijdte van preventie en opsporing.

Buurtinformatienetwerk Haven

Daarnaast zorgt het Buurtinformatienetwerk Haven (BIN) in Antwerpen voor verhoogde waakzaamheid tussen bedrijven in de haven, de scheepvaartpolitie en Port of Antwerp-Bruges. Het netwerk sensibiliseert bedrijven in de haven door onder andere preventieve tips te delen, maar contacteert hen ook telefonisch in geval van dringende situaties.

Alle aangesloten bedrijven zijn automatisch gekoppeld aan het nationale BE-Alert systeem. Zo worden zij bij een noodsituatie in de buurt snel verwittigd.





Trainingen en awareness

Exercitium handboek

Port Facility Security Officers (PFSO's) zijn wettelijk verplicht om binnen hun faciliteit oefeningen en trainingen te organiseren. Om hen hierin te ondersteunen ontwikkelde Port of Antwerp-Bruges in opdracht van de Europese Commissie het handboek Exercitium. Dit handboek biedt kant-en-klare scenario's en ideeën om kleine en grote beveiligingsoefeningen op terminals uit te voeren.

ISPS en Port Security oefeningen

Sinds 2023 organiseren de Port Facility Security Officers van North Sea Port elk jaar een havenbrede, grensoverschrijdende Port Security oefening. Daarbij trainen de PFSO's van zowel Gent als Terneuzen/Vlissingen gelijktijdig hetzelfde scenario. ISPS-faciliteiten krijgen bovendien de mogelijkheid om op datzelfde moment hun eigen jaaroefening te organiseren. Zo kunnen ze op een efficiënte manier ervaringen delen.



Ontdek hier het
Exercitium handboek

Interne ISPS-cursus

De Port Security-afdelingen van Antwerpen en Zeebrugge ontwikkelden een eigen ISPS-basiscursus die de belangrijkste verplichtingen uit de ISPS Code en de Wet Maritieme Beveiliging toelicht. Deze opleiding is bedoeld voor eigen personeel dat dagelijks actief is in het havengebied of op eigen ISPS-gebonden faciliteiten zoals sluizen en cruisterminals werkt.

Cursussen voor bewakingsagenten

Voor bewakingsagenten die worden ingezet bij ISPS-faciliteiten is de cursus 'Havenbewaking – EXE14' verplicht. Zij maken hierin kennis met de haven als werkomgeving, wat ISPS is, hoe havens beveiligd worden en welke bewakingstechnieken er zijn.

Sensibiliseringstraining voor havenwerknemers

Daarnaast bieden verschillende opleidingsverstrekkers specifieke security awareness-trainingen aan. Deze korte trajecten maken medewerkers bewust van risico's, hun gedeelde verantwoordelijkheid en de manier waarop ze correct en tijdig moeten handelen.

In Limburg organiseerde de bedrijfscoördinator van stad Genk een sensibiliseringsronde voor alle bedrijven met watergebonden activiteiten gelegen in Genk-Zuid. Daarnaast werkte de provinciale stuurgroep in 2024 een sensibiliseringscampagne uit voor de bedrijven en havenfaciliteiten van het gebied Genk-Zuid, vooral gericht op bedrijven met 'risicovolle' activiteiten.

CPTED-traject

De stad Genk liet een CPTED-traject (Crime Prevention Through Environmental Design) lopen op het gebied Logistics Valley Flanders. Daarbij brachten ze de aanwezige risico's in kaart van de vele betrokken bedrijven.

Ronselproof-campagnes

Via ronselproof-campagnes, simulaties en trainingen, onder meer in samenwerking met hogescholen en bewakingsondernemingen, leren jongeren en werknemers verdachte toenaderingen herkennen en afwijzen. North Sea Port maakte een security awareness training en ronselproof-training voor ieder personeelslid verplicht. Dat past binnen hun programma rond weerbaarheid. Daarnaast stelt North Sea Port de ronselproof-trainingen actief ter beschikking aan ISPS-terminals.

Jongeren aan de hogescholen die studierichtingen volgen met een link naar de logistieke- en havensector krijgen een specifiek lespakket 'awareness jongeren', uitgewerkt met het Openbaar Ministerie Antwerpen.

Awareness campagne voor havenpersoneel en zeevarenden

DG Scheepvaart en het Nationaal Drugscommissariaat werken aan een landelijke aanpak van corruptie in havens en bij zeevarenden. Dat doen ze via bewustmakingscampagnes en tools op maat om personeel weerbaarder te maken met informatie en oplossingen.

Samenwerken rond beveiliging

“Samenwerking is de sleutel. Niemand kan deze strijd alleen voeren. Politie, justitie, douane, maar ook bedrijven, havenautoriteiten en vakbonden moeten elkaar vinden. Criminelen werken grensoverschrijdend en delen informatie snel. Als wij dat niet doen, lopen we achter de feiten aan.”



Ine van Wymersch
Nationaal Drugscommissaris

Geen enkele haven kan zichzelf beveiligen in isolatie. Daarom werken het parket, douane, havenautoriteiten en private bedrijven steeds nauwer samen in havenregio's. Dat doen ze in gezamenlijke overlegstructuren of multidisciplinaire beveiligingsplatformen. Zowel in samenwerkingen die door een publieke instantie getrokken worden, als publiek-private samenwerkingen. Die zorgen voor een snellere informatie-uitwisseling, gezamenlijke aanpak van georganiseerde misdaad en de uitrol van innovatieve beveiligingstoepassingen.

Lokale netwerken

Publiek-private samenwerkingen op lokaal niveau

Data Community in North Sea Port

Een sterk voorbeeld van publiek-private samenwerking is de Data Community binnen North Sea Port. Dit netwerk verenigt bedrijven in de haven en het havenbedrijf zelf rond één missie: het versterken van het digitale ecosysteem in de nautische en logistieke keten, met beveiliging als centraal thema.

De Data Community werkt rond twee strategische pijlers:

1. Slimme digitale samenwerking in de keten

Door betere data-uitwisseling worden aankomsten, afvaarten en logistieke stromen efficiënter én transparanter.

2. Collectieve aanpak van identiteits- en toegangscontrole

Bedrijven stemmen hun toegangsprocedures op elkaar af, met als doel één uniforme en betrouwbare toegangsstandaard binnen de volledige havenregio.

Deze ambities worden vertaald van pilot naar praktijk via het North Sea Portal, het centrale digitale knooppunt voor veilige data-uitwisseling. De eerste concrete realisatie is de introductie van de Port Pass: een gezamenlijke digitale toegangssleutel met biometrische identificatie, uitgerold bij meerdere grote bedrijven in het Gentse havengebied.

Security Think Tank

De Security Think Tank is een publiek-private samenwerking met vertegenwoordiging van diverse havengebruikers, dienstverleners en autoriteiten. Die komt drie keer per jaar samen om diverse onderwerpen rond ISPS en Port Security te bespreken.

Publiek Private samenwerking Genk

Momenteel is de stad Genk bezig met het uitwerken van een publiek-private samenwerking in de vorm van het opbouwen van een vertrouwensketen, waarbij bedrijven op regelmatige basis gesensibiliseerd worden.

Port Facility Security Officers

North Sea Port organiseert tweejaarlijks ISPS-infosessies voor PFSO's aan beide landszijden. Daarnaast worden in Gent tussentijds ad hoc sessies georganiseerd rond specifieke thema's, met zowel PFSO's als CEO's van ISPS-terminals. Port of Antwerp-Bruges organiseert gelijkaardige sessies voor de PFSO's waar belangrijke info wordt gedeeld en ook ruimte is om te netwerken met elkaar. Daarnaast worden er thema's besproken zoals risico's en dreigingsbeeld, maatregelen en goede praktijken en nieuwe wetgeving. Er komen regelmatig gastsprekers aan bod.

Taskforce Containers

De Taskforce Containers is een nieuw initiatief in Antwerpen om op het vlak van beveiliging best practices, maatregelen en zwakke plekken tussen verschillende terminals te delen in vertrouwelijke kring.

Publieke samenwerkingen op lokaal niveau

Stuurgroep Zone met Globale Notificatie

(GNZ) Defensie organiseert regelmatig oefeningen in Port of Antwerp-Bruges als extra ontradende maatregel. Dat is verankerd in een specifiek protocol waarbij de leden van de Stuurgroep GNZ geïnformeerd worden over de oefeningen en bijkomende voorwaarden kunnen opleggen.

Strategische Tafel Stroomplan 2.0

Het Stroomplan 2.0 is het lokale anti-drugsplan in Antwerpen onder leiding van de procureur des Konings. Het plan zet met diverse acties in op vier assen: barrières in de haven, integrale aanpak, verbeteren van onderzoek en integriteitsbeleid. Gelijkaardige initiatieven zijn opgestart in Limburg en Gent.

Lokaal Comité Maritieme Beveiliging

Het Lokaal Comité Maritieme Beveiliging (LCMB) is de lokale bevoegde autoriteit voor ISPS in elke haven of waterweg met havenfaciliteiten. Het comité komt vier keer per jaar samen of ad hoc als dat nodig is. De samenstelling en werking zijn verplicht door de wet.

Limburg bevindt zich op dit vlak in een unieke positie: er is geen haven, maar er zijn wel verschillende havenfaciliteiten aanwezig. Daarom is er geen volwaardige havenkapiteinsdienst aanwezig. Dat vangen ze op met hun LCMB-werking en door in te zetten op een sterk partnership met de verschillende veiligheidspartners.

Provinciale stuurgroep Limburg

De gouverneur van Limburg nam het initiatief om een provinciale stuurgroep op te richten om best practices over de verschillende havenfaciliteiten heen te identificeren en uit te wisselen.

Nationale netwerken

Nationale Autoriteit Maritieme Beveiliging

De Nationale Autoriteit Maritieme Beveiliging (NAMB) is de nationale bevoegde autoriteit voor ISPS. Ze komt vier keer per jaar samen, of ad hoc als het nodig is. De samenstelling en werking zijn verplicht door de wet.



Europese en Internationale netwerken

Port Security Steering Committee

Het Port Security Steering Committee is een samenwerking tussen de drie grootste havens van Europa: Rotterdam, Antwerpen-Brugge en Hamburg. Daarbij werken ze samen in drie werkgroepen: ISPS-standaarden en innovatieve maatregelen, Modus Operandi en Samenwerking Zuid-Amerika. Er werd ook een Letter of Intent getekend met andere havens uit de Hamburg-Le Havre range om hen op de hoogte te houden van de ontwikkelingen binnen de stuur- en werkgroepen.

European Ports Alliance Public Private Partnership (EPA PPP)

Om de toenemende infiltratie van criminele netwerken in Europese havens tegen te gaan, lanceerde de Europese Commissie onder het Belgisch EU-Voorzitterschap op 24 januari 2024 de EPA PPP. Deze publiek-private samenwerking verenigt alle stakeholders in een gezamenlijke aanpak tegen drugsmokkel en georganiseerde misdaad.

Pan-Atlantic Cooperation

De Pan-Atlantic Cooperation is een samenwerking tussen de bevoegde ISPS-autoriteiten van de 3 grootste EU havens en Colombia, Ecuador en Peru. Daarbij gebruiken ze ISPS als bindmiddel om goede praktijken rond preventie en beveiliging van havens te delen en verbeteren.

Perimeter en toegang

“De maritieme beveiliging van onze havenfaciliteiten draagt bij aan het verbinden van regio's, het versterken van de economie en het bouwen aan duurzame ontwikkeling. Strikte toegangscontrole en registratie, zoals via ItsMe[®], zijn daarbij essentieel om de integriteit van onze logistieke keten te garanderen. Zo versterken we de veiligheid en de efficiëntie van onze havenfaciliteiten.”



Robin Minten

Voorzitter LCMB Limburg en
directeur-coördinator Federale Politie Limburg

Perimeter en toegang

Een robuuste beveiliging begint aan de poort. Belgische havens en havenfaciliteiten investeren daarom in moderne toegangs- en perimeteroplossingen die zowel adequaat als gebruiksvriendelijk zijn.

Digitale platformen, slimme identificatiemiddelen en innovatieve infrastructuur zorgen ervoor dat enkel geautoriseerde personen de juiste zones kunnen betreden en dat elke toegang traceerbaar en controleerbaar blijft.

Digitale toegangscontrolesystemen

Alfapass

Alfapass is een systeem voor digitale identificatie en autorisatie in de haven van Antwerpen-Brugge. Via één gecentraliseerde badge kunnen werknemers, bezoekers en dienstverleners zich identificeren aan terminals en faciliteiten. Het initiatief groeide vanuit de noden van de private sector. Diverse spelers maken ondertussen gebruik van het systeem dankzij de eenvoudige integratie met bedrijfsprocessen en poortsystemen.

Prean

Prean is een self-serviceplatform voor vooraanmeldingen van bezoekers aan schepen en havenlocaties. Hoewel Prean zelf geen toegang verleent, centraliseert het alle noodzakelijke informatie om te beslissen of iemand toegang krijgt tot een locatie en vereenvoudigt het bezoekersbeheer voor bedrijven, agenturen en havenfaciliteiten.

Peripass

North Sea Port bouwt aan een uniforme oplossing via Peripass, een yard management- en toegangsplatform dat in samenwerking met de ISPS-faciliteiten wordt uitgerold als centrale Port Pass. Deze oplossing combineert planning, toegangscontrole en logistieke flow in één systeem en is het eerste concrete resultaat van hun Data Community.

ItsMe®

De Limburgse havenfaciliteit Port of Limburg toont aan dat ook binnenhavens vooroplopen in technologische beveiliging. Als één van de best beveiligde binnenhavens van de Benelux werkte het samen met SCR en ItsMe® om een digitaal identificatieproces te implementeren dat voldoet aan de strengste normen.

Slim hekwerk

Naast digitale oplossingen wordt ook de fysieke beveiliging slimmer. Een slim hekwerk wordt uitgerold in Port of Antwerp-Bruges. Deze infrastructuur is uitgerust met detectiesensoren en zorgt in samenwerking met cameratechnologie en real-time monitoring voor een maximale bescherming tegen indringingspogingen.

North Sea Port zet in op slim hekwerk, met de aanleg van drie kilometer hekwerk als bijkomende verdedigingslijn tegen criminaliteit.

Port of Limburg heeft detectiesensoren en thermische camera's die de gehele perimeter/omheining afdekken. Die versturen elke intrusie meteen naar de gsm van de verantwoordelijken.





Detectie

Detectie is belangrijk voor een veilige en vlot functionerende haven. Met de Central Control Room in Zeebrugge brengen we data van heel wat actoren samen om efficiënter te monitoren en samen te werken. De inzet van havenbrede slimme camera's draagt daaraan bij, door risico's vroeg te detecteren en te analyseren. Zo versterken we de veiligheid van mensen, infrastructuur en scheepvaart."



Kim Pettens

Voorzitter LCMB Zeebrugge en
havenkapitein bij Port of Antwerp-Bruges

Detectie

Een moderne haven is niet alleen een logistieke draaischijf, maar ook een specifieke hoogbeveiligde zone waar elk risico vroegtijdig moet worden opgemerkt. Daarom investeren Belgische havens in een uitgebreid detectienetwerk dat land, water en lucht combineert. Van een geavanceerd radarnetwerk tot slimme camera's en drones: technologie fungeert als de ogen en oren van het havengebied.

Gecentraliseerde monitoring vanuit controlekamers

Vessel Traffic Center

Het Vessel Traffic Center vormt de ruggengraat van het maritieme toezicht. Het is een gecentraliseerde controlekamer die waakt over het scheepvaartverkeer. Via uitgebreide radar- en camerasystemen houden Vessel Traffic Services (VTS) voortdurend zicht op de scheepvaart in en rond de havenzones. In Antwerpen gebeurt dit vanuit het Antwerp Coordination Center (ACC).

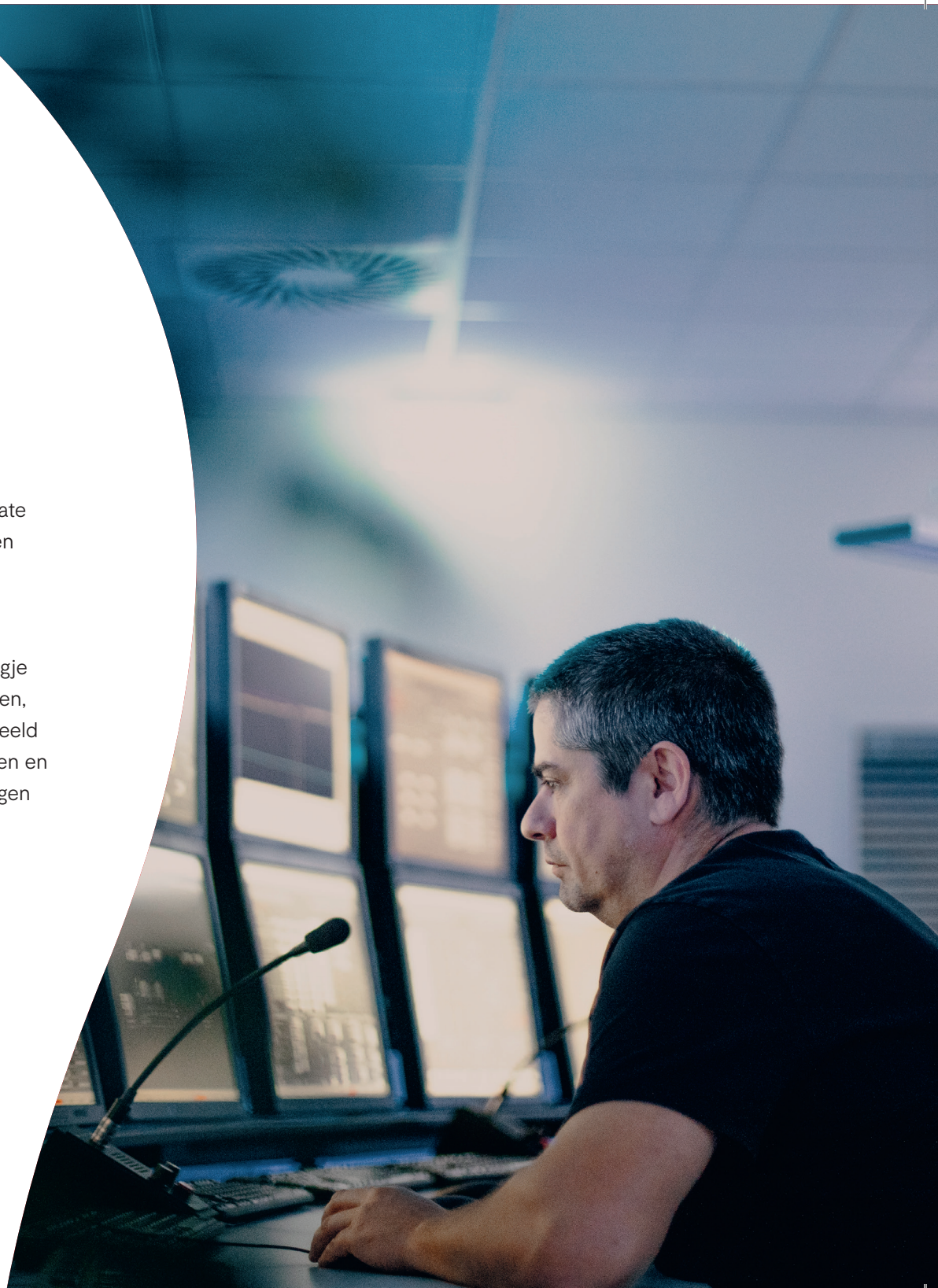
Central Control Room

In Zeebrugge werd de Central Control Room (CCR) ingericht. Die verbetert de communicatie, veiligheid en beveiliging van de activiteiten in de haven. Honderden camera's van beveiligingsdiensten van private bedrijven sluiten aan op de controlekamer, waar al die beelden gemonitord worden.

AI-gedreven cameranetwerken

Bij Antwerpse terminals en in North Sea Port staat een uitgebreid netwerk van vaste en mobiele ANPR-camera's (Automatic Number Plate Recognition). Deze systemen registreren nummerplaten van voertuigen aan poorten, wegen en terminals en koppelen die automatisch aan toegangsrechten of risicoprofielen.

Daarnaast houden slimme camera's met artificiële intelligentie een oogje in het zeil in Antwerpen en Zeebrugge. De camera's herkennen schepen, bieden ondersteuning bij de opvolging van incidenten en kunnen gedeeld worden met beveiligingsdiensten. De slimme camera's sporen personen en problemen in het verkeersnetwerk snel en gemakkelijk op en verwittigen meteen de centrale controlekamer.



Drones

Het luchtruim wordt steeds belangrijker in detectie. In Antwerpen is een permanent dronenetwerk actief waarmee inspecties, observaties en noodinterventies vanuit de lucht kunnen worden ondersteund. North Sea Port zet drones in voor inspecties, met aanvullende dronedetectie in ontwikkeling om ongewenste toestellen tijdig te onderscheppen. Op het dak van Port of Limburg staat een “drone in the box”. De lokale politie gebruikt die bij incidenten in het gebied Genk-Zuid, waar het gros van de Limburgse havenfaciliteiten gelegen zijn.

In Zeebrugge staat een dronedetectieplatform, waarmee de Central Control Room 24/7 het luchtruim monitort. Daarbij houden ze rekening met externe dreigingen zoals klimaatactivisme, aanwezige NAVO of niet-NAVO militaire schepen, etc.

Mobiele scanners

Tot slot versterken mobiele containerscanners van de douane het detectiearsenaal. Deze apparatuur maakt het mogelijk om snel, lokaal en gericht goederen te controleren zonder grote logistieke vertraging. Ze besparen een verplaatsing van de container, onder begeleiding, naar een Grens Inspectie Post en zorgen zo voor een efficiëntere en snellere scanningsprocedure.





Patrouillevaartuigen

Op het water zorgen zowel de Scheepvaartpolitie als de havenbedrijven voor zichtbare aanwezigheid via moderne patrouillevaartuigen. De Scheepvaartpolitie heeft recent nieuwe vaartuigen in gebruik genomen die ze zowel in de havens als vaarwegen naar de havens inzetten.

Zo beschikt de Scheepvaartpolitie in Gent over een patrouillevaartuig voor het havengebied en een snel interventievaartuig. Ook Port of Antwerp-Bruges nam in 2022 twee nieuwe handhavingsvaartuigen in gebruik. In de haven van Antwerpen kan de Scheepvaartpolitie twee patrouillevaartuigen en een snel interventievaartuig inzetten. Met de oprichting van een post van de scheepvaartpolitie in Limburg in 2023, werd er in 2024 ook een nieuw patrouillevaartuig in gebruik genomen.

Havenbeveiliging

Omwille van het nationale belang van de Antwerpse haven zet de Scheepvaartpolitie naast de reguliere interventieploegen ook een specifiek havenbeveiligingsteam in. Zij beveiligen de haven als vitale infrastructuur tegen terroristische en criminele organisaties.



Andere beveiligings- projecten

Naast fysieke bewaking en toegangscontrole investeren Belgische havens ook in vernieuwende systemen die de beveiliging in elke schakel van de logistieke keten versterken, zowel op de terminal zelf als in de digitale omgeving.

Certified Pick-Up: controle tot aan de containerdeur

Met Certified Pick-Up introduceerde Port of Antwerp-Bruges een volledig digitaal en beveiligd vrijgavemechanisme voor containers. Waar vroeger papieren documenten of pincodes werden gebruikt, werkt het systeem nu via een geïntegreerde, identiteitsgebonden autorisatieketen. Enkel de correct geregistreerde vervoerder krijgt toegang tot de container op het moment van afhaling.

Het resultaat: minder fraude, minder misbruik van pincodes en volledige traceerbaarheid van elke overdracht. Na één jaar waren al meer dan één miljoen containers via dit systeem vrijgegeven — een duidelijke indicatie van de brede aanvaarding binnen de sector.

Ook Port of Limburg zorgt voor een veilig containerafhaalproces met het Secured Container Release-systeem van T-Mining, gekoppeld aan ItsMe®.



Digital Twins: het virtuele zicht op de werkelijkheid

Om sneller en accurater te reageren op incidenten, bouwen havens aan Digital Twin-platformen (zoals APICA in Port of Antwerp-Bruges). Deze digitale kopieën van het havengebied combineren real-time data uit sensoren, camera's, verkeerssystemen en weersinformatie.

Zo krijgen operators een “derde oog” op het terrein, waarmee ze zowel dagelijkse operaties als noodsituaties efficiënter kunnen monitoren en simuleren. Digital Twins groeien daarmee uit tot strategische tools voor incidentdetectie, planning en risico-analyse.

Cyber resilience

Digitale weerbaarheid is even essentieel als fysieke beveiliging. Daarom rollen verschillende havens programma's rond cyber resilience uit.

Bij Port of Antwerp-Bruges is de afdeling Cyber Resilience verantwoordelijk voor de digitale veiligheid en weerbaarheid van de organisatie. De afdeling zorgt er niet enkel voor dat de ICT-systemen veilig blijven, maar ook dat de hele organisatie voorbereid is op cyberdreigingen. Ze houden voortdurend de vinger aan de pols door de ICT-omgeving te monitoren op onregelmatigheden en verdachte activiteiten. Daarnaast ontwikkelen ze het cyberbeleid, de strategie en de processen die de basis vormen van de cyberweerbaarheid van Port of Antwerp-Bruges.

Het team beheert en implementeert cybersecuritytechnologieën, volgt de NIS2-wetgeving op de voet, en werkt actief mee aan het vergroten van de weerbaarheid van de organisatie. Ook het versterken van de cybersecuritycultuur binnen de organisatie is een belangrijke pijler. Tenslotte zetten ze sterk in op samenwerking buiten de organisatie, onder meer via de Belgian Ports ISAC, waar ze met andere havenbedrijven informatie delen over dreigingen en best practices.

North Sea Port werkt samen met andere Nederlandse zeehavens aan een landelijk cybersecurityplatform, onder coördinatie van overheid en beveiligingsdiensten. Via kennisdeling, gezamenlijke dreigingsanalyse en training worden bedrijven in de havenketen weerbaarder gemaakt.

Initiatieven zoals de inspiratiesessie “Cyber Resilience in de Haven” van Alfaport Voka tonen hoe sensibilisering en samenwerking de sleutel vormen om de digitale verdedigingslijn even sterk te maken als de fysieke.



Port 2 Port

Security Platform