Port 2 Port

Security Platform

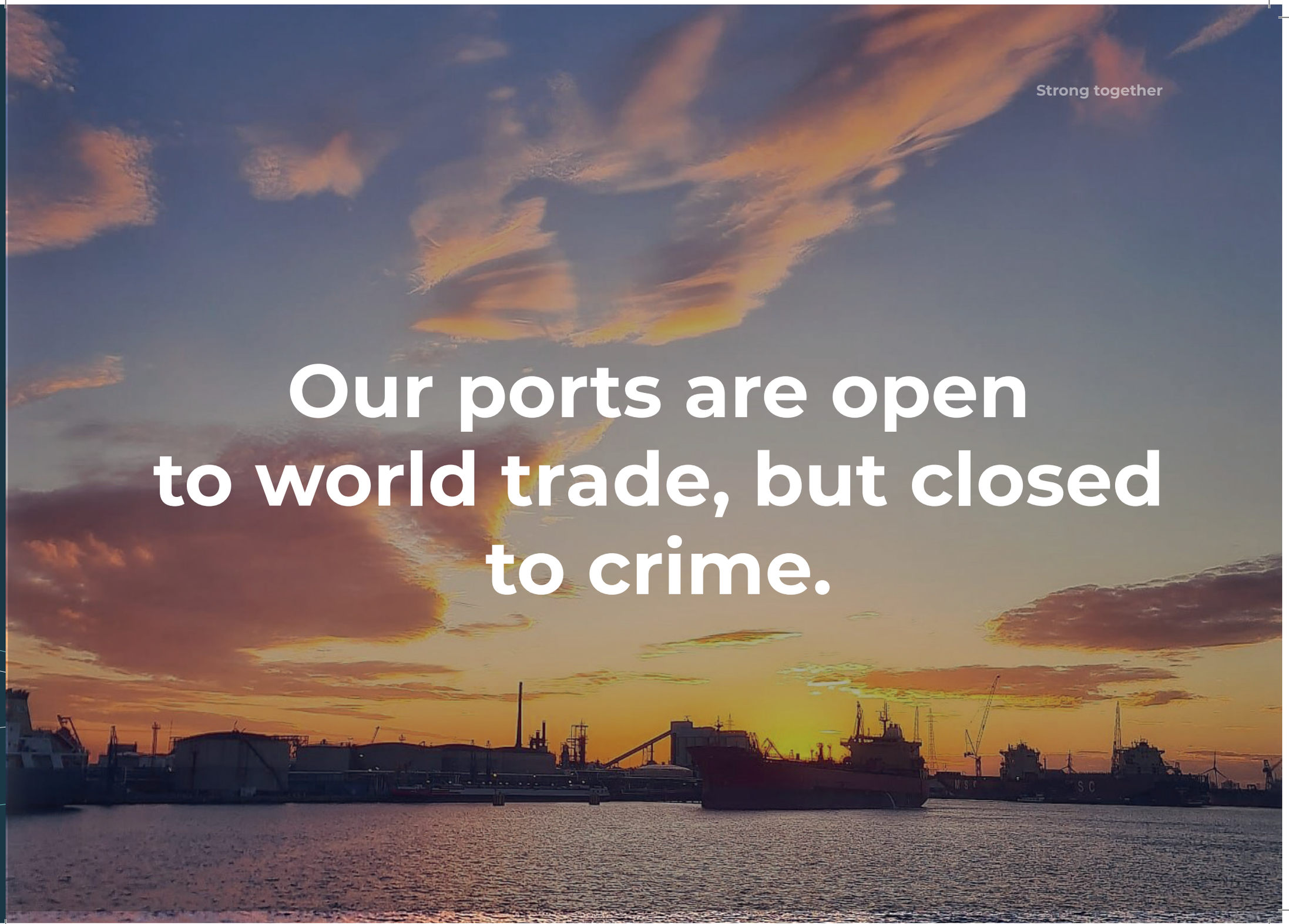

Lenovo
Port Authority
North Sea Port
Together Smarter

Content

Strong together

Belgian ports are gateways to the world. They connect people, goods and industry, but where these flows come together, there are also risks. Today more than ever, organised crime and cross-border threats call for a joint, integrated approach. There were therefore growing calls from various ports to combine best practices in the area of security and provide for structural cooperation. This shared ambition formed the basis for the Port 2 Port Security Platform.

Port 2 Port Security Platform is a joint initiative of Port of Antwerp-Bruges, North Sea Port and Federal Police CSD Limburg, in close cooperation with the National Drug Commission. The platform, launched on 21 November 2025, unites all Belgian seaports and inland ports. A new step to make our ports more resilient in a constantly changing society.



Our ports are open to world trade, but closed to crime.

The appointment of Ine Van Wymersch as the first National Drug Commissioner means that Belgium now has a single point of contact in the fight against organised crime and drug-related crime. Through her role, Ine and her colleagues at the National Drug Commission are building an integrated, national strategy that unites the police, judiciary, ports, businesses and citizens around one goal: to make our society and economic gateways resilient to criminal infiltration. This approach was concretised in the Iceberg Strategy.

Collaboration is not an option, but a necessity

Our ports are economic engines at the global level," explains Ine Van Wymersch. "Every day thousands of people, goods and ships pass through them. This large-scale dynamic is a strength, but at the same time a vulnerability. Criminal organisations try to infiltrate this logistics chain – often subtly, through technology or the gullible weakest links."

In Van Wymersch's view, collaboration is the key. "No-one can fight this battle alone. The police, judiciary, customs, as well as companies, port authorities and trade unions must come together. Criminals are not confined by borders and share information quickly. If we don't take the same approach, we will be one step behind."

She emphasises that good practices and insights must not remain within one port. "What works today in Antwerp or Ghent can make a difference tomorrow in Limburg, Liege or Brussels. We must share our knowledge or we will lose precious time. Port authorities play a crucial role in this regard: they connect the public and private worlds."

The Iceberg Strategy: chipping away at the iceberg AND warming the temperature of the water

Van Wymersch likes to use the metaphor of an iceberg to describe the national approach. “The criminal organisations are the iceberg. What we see are the drug busts, shootings and explosions. But that’s just the tip of the iceberg,” she explains. “Below the waterline is the much larger, invisible part: money laundering, corruption, blackmail, and abuse of staff. If we only chip away directly at the iceberg, based on enforcement, but do not act on the temperature of the water, by increasing the resilience of organisations and workers, our ecosystem will stay in the cold. And if it’s cold, the criminal iceberg won’t melt.”

That is why the Iceberg strategy combines two approaches. “On the one hand, we have the direct approach: the police, judiciary and customs who are taking decisive action (or chipping away at the ice). On the other hand, we are investing in the indirect approach: prevention, training, awareness, resilience. If we train our people, strengthen HR policies and organise information sharing, this will heat up the water. This will melt the iceberg and the direct approach will also become much more effective.”

One ecosystem, one responsibility

For Van Wymersch, it is clear that security does not stop at the gateway to the port.

“Shipping companies, terminals, logistics companies, trade unions, governments and international partners – they are all part of the same ecosystem. If one party is outside this network, it creates room for crime. Only through collaboration and open communication can we close this gap.”

She urges all parties involved not to wait for others. “The future demands action, not a wait-and-see approach. Each port authority can make a difference by sharing information, identifying the risks and using the iceberg strategy as a common compass. That way, we can make our ports not only economic hubs, but also places where fair competition, enforcement and resilience go hand in hand.”

Legislation & inspections

“The revised Maritime Security Act has pushed security standards at our port to a new level. This Act means that we can detect risks more quickly and take more effective action against criminal activity. It allows us to structurally reinforce the security of people, property and infrastructure. This is essential for a reliable and forward-looking port.”

Niels Vanlaer
Chairperson LCMB Antwerp and
port captain Antwerp at Port of Antwerp-Bruges

Port security is not a patchwork of individual measures, but builds on a solid international framework in the form of the ISPS Code, supplemented by national legislation and local initiatives. In this regard, Belgium is among the forerunners in Europe, with its Maritime Security Act.

ISPS: A shared security standard

The basis for maritime security is laid down in the International Ship & Port Facility Security Code (ISPS). This global standard is mandatory for passenger ships sailing internationally, cargo ships with a gross tonnage of 500 tons or more, mobile offshore drilling platforms and port facilities receiving these ships.

To identify security risks and take effective measures, Port Facility Security Assessments and Port Facility Security Plans are required by law. These include procedures for access control, surveillance, loading monitoring and incident and exercise guidelines.

In addition to putting in place security infrastructure and procedures, the ISPS Code also provides a framework for (inter)national cooperation between public and private actors in the maritime sector.

Belgium shows ambition with the Maritime Security Act

The security measures from the ISPS have been incorporated into the European Regulation (725/2004). Belgium transposed these international provisions into national legislation through its Maritime Security Act, incorporated into the Belgian Shipping Code. This Act uses the framework of the ISPS code to tackle organised crime, whereby the framework, structure and capabilities available to government and companies have been expanded.

The Act has already undergone two revisions, in 2022 and 2024, raising security standards even higher. In this way, the Act makes more things possible in the area of port security. It strengthens the security of ports and port facilities, and emphasises prevention of illegal activities such as drug smuggling and human trafficking. At the same time, it protects vital infrastructure, personnel and facilities from unlawful acts.

The Belgian legislation introduces a series of innovative measures that help ensure a modern, integrated security approach:

Special extract from the criminal record: with this new document, employers can check the criminal background of individuals who want to work in the port or at port facilities.

Port bans via the AIGIS platform: through the AIGIS platform, the Act provides for the possibility of monitoring port bans. This is a punishment for violating drug laws and other criminal offences.

Security verifications via the PANOPTES platform: the PANOPTES platform makes it possible to carry out the mandatory security verification of individuals with critical functions in the port or port facilities, such as those with access to certain companies, assets, IT systems, personnel policies, port information, etc.

Use of biometrics and smart cameras: an extension of the legal framework for advanced access control and camera surveillance in the port, port facilities and on the Belgian part of the North Sea.

Risk-based security: inland navigation terminals and companies with an impact on maritime security can also be subject to various minimum requirements regarding security, based on a risk analysis.

Discover the AIGIS-platform

Competent ISPS authorities

The revised Maritime Security Act provides a structural and automated approach to security in Belgian ports and port facilities. The Act improves cooperation and information exchange between the various agencies such as the Local Police, DG Shipping, Waterway Police, Customs, Defence, National Crisis Centre, State Security, General Intelligence and Security Service, Coordination Unit for Threat Analysis, the ports (Port Security Officers), Maritime Security Unit, Provincial Command and the Regions.

The National Authority for Maritime Security (NAMB), chaired by the FPS Mobility and Transport, is responsible for implementing and developing the Act. For daily follow-up, NAMB is supported by the Maritime Security Unit (CMB).

In every port or waterway with port activity, there is a Local Committee for Maritime Security (LCMB). There are 9 LCMBs in Belgium in total. Together with the CMB, these coordinate the practical implementation of ISPS in their port area. An LCMB is an effective and unique platform where key security partners from the port area come together. As it is a local committee, the people at the table are primarily those who know the area inside out. As all participants have security clearance, sensitive information can be shared securely and confidentially.

Knowledge sharing as a lever for quality

Port of Antwerp-Bruges, Rotterdam and Hamburg developed a joint standard to improve ISPS perimeter and access controls. This allows authorities and port operators to specify security measures based on an agreed risk standard. This standard has since been made mandatory in Belgium as well.

Local initiatives

Besides international standards, local initiatives play an important role in strengthening ISPS security. As such, ports can also individually go a step further. Through the port police regulation, Port of Antwerp-Bruges and North Sea Port make access control measures mandatory for all companies in the port area. As a result, security is no longer limited to strictly ISPS-compliant sites.

In Limburg, the provincial steering committee is developing a similar police regulation with the city of Genk.

In North Sea Port (Ghent), port lieutenants also conduct interim ISPS inspections based on their own local checklist. They use an in-house-developed application in this regard, which ensures structured planning and monitoring. At Port of Antwerp-Bruges, a team of Port Authority Officers is on hand to keep an eye on things on a daily basis and report security issues to the LCMB.

Discover the ISPS port security standards in this brochure

Security-related websites

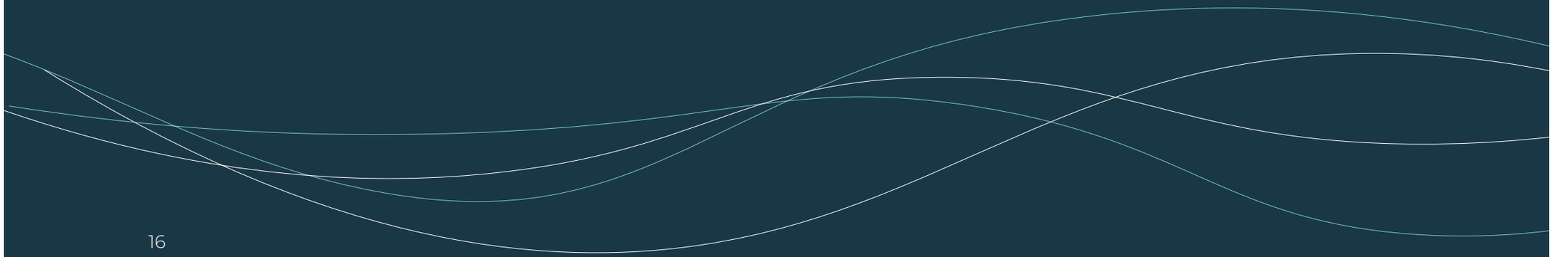
For more information, visit the ISPS and port security websites of the Belgian Ports:

Port of Antwerp-Bruges

North Sea Port

DG Shipping

Reporting points and training



Awareness is our first line of defence against crime. It is important to ensure this alertness among everyone in or around the port. For example, with criminal recruitment-proof training, we teach our staff and young people how to recognise and deter criminal recruitment attempts. Reporting points like Portwatch then make it easy to report suspicious situations anonymously. In this way, we strengthen the resilience and integrity of our port together."

Wim Van Bogaert
Chairperson LCMB Gent and
port captain North Sea Port

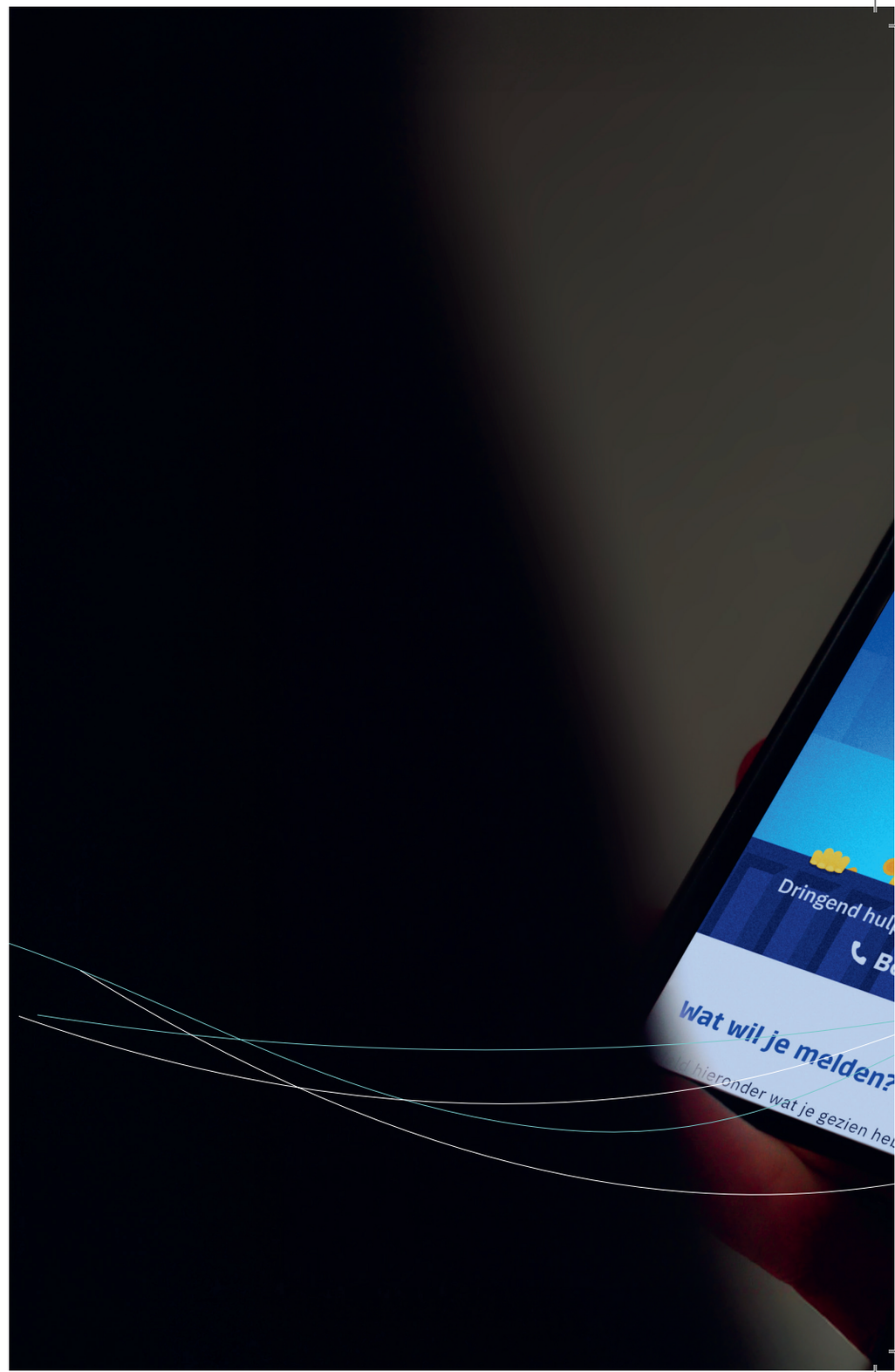
Reporting platforms, awareness campaigns and targeted training are combined to form an integrated security and awareness approach. This ensures that we detect and address abuse, crime and risks early.

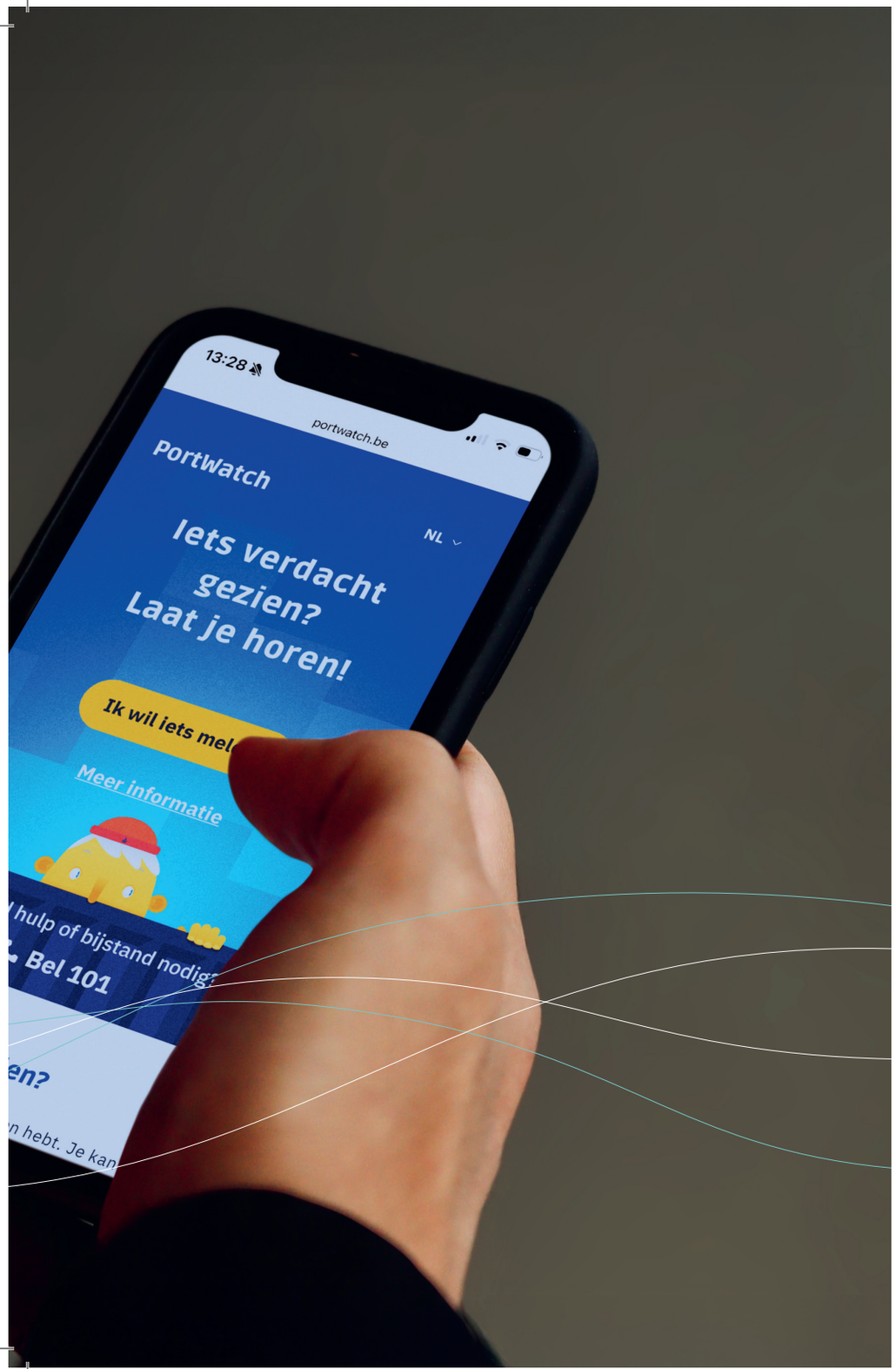
A resilient port community

Belgian ports and port facilities are investing heavily in continuous training, joint exercises and targeted awareness-raising. In this way, they intend to make staff resilient to criminal influences and able to identify risks in time. Both operational personnel and managers are actively involved in a learning security network. There are also several reporting points where suspicious situations can be reported immediately to the appropriate body.

Discover Portwatch

Discover Our Port Drug-Free





Anonymous reporting points as the first line of defence

Portwatch
Portwatch is an anonymous, centralised reporting point for all Belgian ports and port facilities. Through this online portal, staff, visitors or local residents can easily report suspicious situations. One unique system for the entire country.

Our Port Drug-Free
In Port of Antwerp-Bruges, the platform Our Port Drug-Free is an additional reporting point specifically for Antwerp. Anonymous reports of suspicious behaviour in the context of drug crime can be reported here. The reporting point is complementary to Portwatch: both reporting points reinforce each other and expand the scope of prevention and detection.

Port Neighbourhood information network
In addition, the Port Neighbourhood Information Network (BIN) in Antwerp ensures heightened vigilance between companies in the port, the waterway police and Port of Antwerp-Bruges. The network raises awareness among companies in the port by sharing preventive tips, among other things, but also contacts them by phone in the event of urgent situations.

All affiliated companies are automatically connected to the national BE-Alert system. That way, in the event of an emergency in the area, they are quickly alerted.

Training and awareness

Exercitium handbook

Port Facility Security Officers (PFSOs) are required by law to conduct exercises and training within their facility. To support them in this regard, Port of Antwerp-Bruges developed the Exercitium handbook on behalf of the European Commission. The handbook provides ready-to-use scenarios and ideas for conducting small and large-scale security exercises at terminals.

ISPS and Port Security exercises

Every year since 2023, the Port Facility Security Officers at North Sea Port have organised a port-wide, cross-border Port Security exercise. As part of this, the PFSOs of both Ghent and Terneuzen/Vlissingen train for the same scenario at the same time. ISPS facilities also get the opportunity to host their own annual exercise at the same time, to efficiently share experiences.

Discover the Exercitium handbook here

Internal ISPS course
The Port Security departments of Antwerp and Zeebrugge have developed their own ISPS basic course that explains the main obligations of the ISPS Code and the Maritime Security Act. This course is designed for in-house staff working on a daily basis in the port area or at in-house ISPS-related facilities such as locks and cruise terminals.

Courses for security guards
For security guards deployed to ISPS facilities, the course 'Port Security - EXE14' is mandatory. As part of the course, staff are introduced to the port as a working environment, what ISPS is, how ports are secured and what surveillance techniques are available.

Awareness training for port staff
In addition, several training providers offer specific security awareness training. These short programmes make staff aware of risks, their shared responsibility and the right action to take, in good time.
In Limburg, the business coordinator of the city of Genk organised an awareness session for all companies with water-related activities located in Genk-Zuid. In addition, the provincial steering committee drew up an awareness campaign for the companies and port facilities of the Genk-Zuid area in 2024, primarily aimed at companies with 'high-risk' activities.

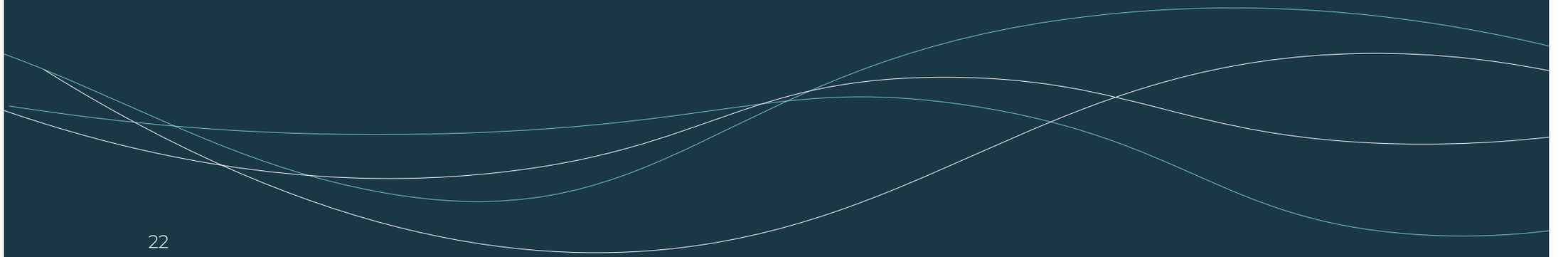
CPTED programme
The city of Genk implemented a CPTED (Crime Prevention Through Environmental Design) programme in the Logistics Valley Flanders area. In so doing, they mapped the risks facing in the many companies involved.

Criminal recruitment-proof campaigns
Through criminal recruitment-proof campaigns, simulations and training, including in collaboration with colleges and security firms, young people and workers learn to recognise and deter suspicious approaches.

North Sea Port made security awareness training and criminal recruitment-proof training mandatory for every staff member. This is part of their programme on resilience. North Sea Port is also actively making criminal recruitment-proof training available at ISPS terminals.
Young people at the colleges studying subjects with a link to the logistics and port sector are taught a specific component on 'youth awareness', developed with the Antwerp Public Prosecutor's Office.

Awareness campaign for port staff and seafarers
DG Shipping and the National Drug Commission are working on a nationwide approach to corruption in ports and among seafarers. This is through awareness campaigns and tailored tools to make staff more resilient with information and solutions.

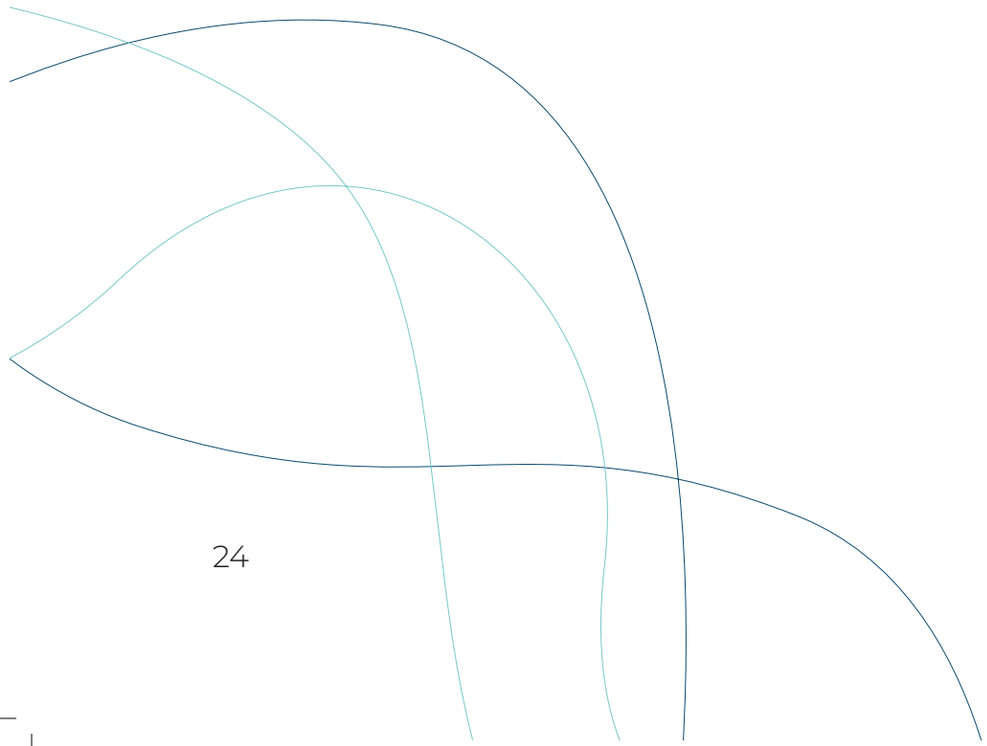
Collaboration around security



“Collaboration is the key. “No-one can fight this battle alone. Police, judiciary, customs, as well as companies, port authorities and trade unions must come together. Criminals are not confined by borders and share information quickly. If we don’t take the same approach, we will be one step behind.”

Ine van Wymersch
National Drug Commissioner

No port can make itself secure in isolation. That is why the public prosecutor's office, customs, port authorities and private companies are increasingly working closer together in port regions. This is in joint consultation structures or multidisciplinary security platforms. Either in collaborations led by a public body or public-private partnerships. These collaborations ensure faster information exchange, joint tackling of organised crime and the rollout of innovative security applications.



Local networks

Public-private partnerships at the local level

Data Community in North Sea Port

An excellent example of public-private collaboration is the Data Community within North Sea Port. This network unites companies in the port and the port authority itself around one mission: to strengthen the digital ecosystem in the nautical and logistics chain, with security as the main theme.

The Data Community works around two strategic pillars:

1. **Smart digital collaboration in the chain**
   Thanks to better data exchange, arrivals, departures and logistics flows become more efficient and transparent.
2. **Collective approach to identity and access control**
   Companies coordinate their access procedures with the goal of a single uniform and reliable access standard across the entire port region.

These ambitions are being translated from pilot to practice via the North Sea Portal, the central digital hub for secure data exchange. The first concrete realisation is the introduction of the Port Pass: a joint digital access key with biometric identification, rolled out in several major companies in the Ghent port area.

Security Think Tank
The Security Think Tank is a public-private partnership with representation from various port users, service providers and authorities. It meets three times a year to discuss various topics related to ISPS and Port Security.

Public Private Partnership Genk
The city of Genk is currently developing a public-private partnership by building a chain of trust, where awareness is raised among companies on a regular basis.

Port Facility Security Officers
Every two years, North Sea Port organises ISPS info sessions for PFSOs in both regions of the country. In addition, ad hoc sessions on specific topics are organised in Ghent, with both PFSOs and CEOs of ISPS terminals. Port of Antwerp-Bruges organises similar sessions for the PFSOs where important information is shared and there is also the possibility to network. In addition, themes such as risks and threat perception, measures and best practices and new legislation are discussed. Guest speakers are regularly invited.

Taskforce Containers
The Containers Taskforce is a new initiative in Antwerp to confidentially share best practices, measures and vulnerabilities in the area of security between different terminals.

Public-private partnerships at the local level

Global Notification Zone (GNZ) Steering Committee
Defence regularly organises exercises in Port of Antwerp-Bruges as an additional deterrent. This is embedded in a specific protocol whereby the members of the GNZ Steering Committee are informed of the exercises and can impose additional conditions.

Strategic 'Tafel Stroomplan 2.0
This is the local anti-drug plan in Antwerp led by the public prosecutor. With various actions, the plan focuses on four strands: barriers at the port, an integrated approach, improving research and integrity policy. Similar initiatives have been started in Limburg and Ghent.

Local Committee for Maritime Security
The Local Committee for Maritime Security (LCMB) is the local competent authority for ISPS in any port or waterway with port facilities. The committee meets four times a year, or ad hoc as needed. Here too, the composition and operations are required by law.

Limburg is in a unique position in this regard: it does not have a port, but it does have several port facilities. There is therefore no full-fledged port captaincy in attendance. The operations of the LCMB make up for that fact, together with a focus on strong partnerships with the various security partners.

Limburg Provincial Steering Committee
The governor of Limburg took the initiative to set up a provincial steering committee to identify and exchange best practices across port facilities.

National networks

National Authority for Maritime Security
The National Authority for Maritime Security (NAMB) is the national competent authority for ISPS. The authority meets four times a year, or ad hoc as needed. The composition and operations are required by law.

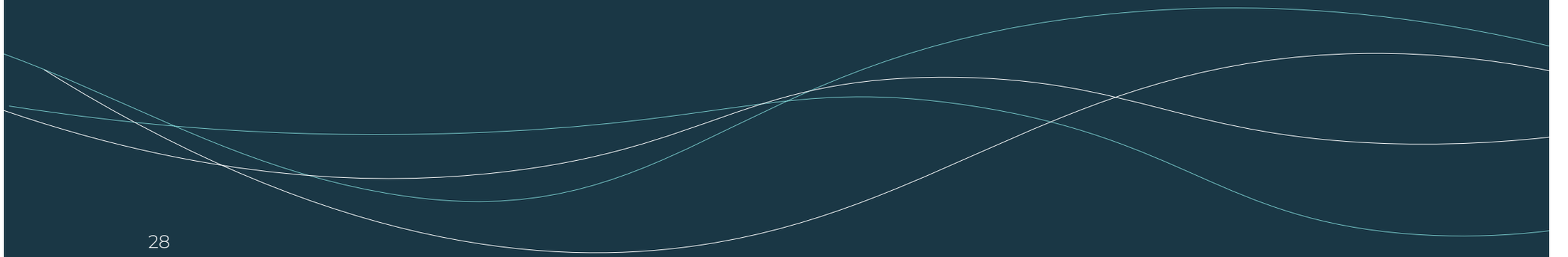
European and International networks

Port Security Steering Committee
The Port Security Steering Committee is a collaboration between Europe's three largest ports: Rotterdam, Antwerp-Bruges and Hamburg. They collaborate in three working groups in this regard: ISPS Standards and Innovative Measures, Modus Operandi and Cooperation South America. A Letter of Intent was also signed with other ports in the Hamburg-Le Havre range to keep them informed of developments within the steering committees and working groups.

European Ports Alliance Public Private Partnership (EPA PPP)
To combat the increasing infiltration of criminal networks into European ports, the European Commission under the Belgian EU Presidency launched the EPA PPP on 24 January 2024. This public-private partnership unites all stakeholders in a joint approach against drug smuggling and organised crime.

Pan-Atlantic Cooperation
The Pan-Atlantic Cooperation is a collaboration between the competent ISPS authorities of the 3 largest EU ports and Colombia, Ecuador and Peru. The ISPS is the connecting factor in this regard, to share and improve good practices in the area of port prevention and security.

Perimeter and access



The maritime security of our port facilities helps connect regions, strengthen the economy and build sustainable development. Strict access control and registration, such as through ItsMe®, are essential in this regard to ensure the integrity of our supply chain. In this way, we are strengthening the security and efficiency of our port facilities.”

Robin Minten
Chairperson LCMB Limburg and
director-coordinator of the Federal Police Limburg

Robust security starts at the gateway. Belgian ports and port facilities are therefore investing in modern access and perimeter solutions that are both up to the challenge and user-friendly.

Digital platforms, smart identification systems and innovative infrastructure ensure that only authorised individuals can enter the right areas and that every access is traceable and verifiable.

Digital access control systems

Alfapass
Alfapass is a system for digital identification and authorisation in the port of Antwerp-Bruges. One centralised badge allows staff, visitors and service providers to identify themselves at terminals and facilities. This initiative grew from the needs of the private sector. Various players are now using the system thanks to its easy integration with business processes and gate systems.

Prean
Prean is a self-service platform for advance notification of visitors to ships and port locations. Although Prean itself does not grant access, it centralises all the necessary information to decide whether to allow an individual access to a location, while simplifying visitor management for companies, agencies and port facilities.

Peripass
North Sea Port is also building a unified solution through Peripass, a yard management and access platform rolled out as a central Port Pass in cooperation with ISPS facilities. This solution combines planning, access control and logistics flow in one system and is the first concrete result of their Data Community.

ItsMe®
The Port of Limburg facility is proving that inland ports are also at the forefront of technological security. As one of the most secure inland ports in the Benelux, it worked with SCR and ItsMe® to implement a digital identification process that meets the strictest standards.

Port of Limburg also has detection sensors and thermal cameras in place that cover the entire perimeter/fence. These immediately send an alert of any intrusion to the GSM of the responsible parties. The latter can directly view images from the cameras on their GSMs.

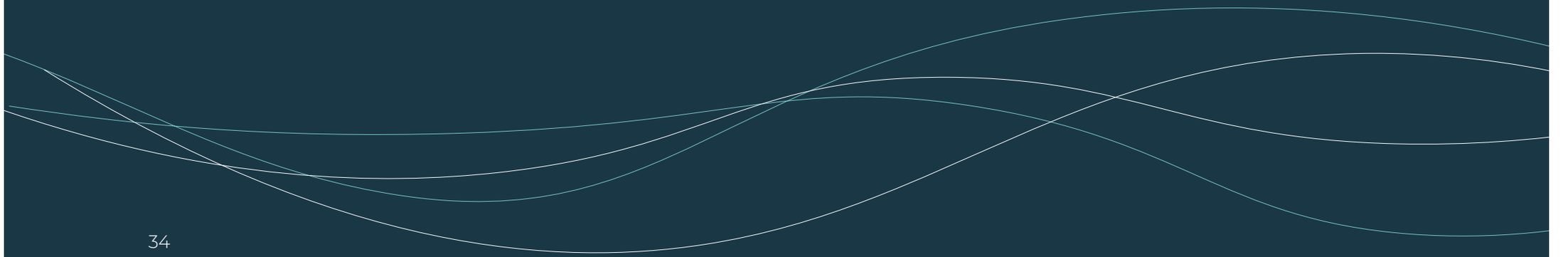
Smart perimeter fencing

In addition to digital solutions, physical security is also getting smarter. Smart perimeter fencing is being rolled out in Port of Antwerp-Bruges. This infrastructure features detection sensors and, in conjunction with camera technology and real-time monitoring, ensures maximum protection against attempted intrusion.

North Sea Port is also focusing on smart perimeter fencing, by installing 3 kilometres of fencing as an additional line of defence against crime.

Port of Limburg also has detection sensors and thermal cameras in place that cover the entire perimeter/fence. These immediately send an alert of any intrusion to the GSM of the responsible parties. The latter can directly view images from the cameras on their GSMs.

Detection



Detection is essential for a safe and smoothly functioning port. With the Central Control Room in Zeebrugge, we bring together data from various security services to monitor and work together more efficiently. Our smart cameras also make a contribution in this regard, by detecting risks and immediately alerting the Central Control Room. In this way, we are ensuring that people, infrastructure and shipping are safer."

Kim Pettens
Chairperson LCMB Zeebrugge and
port captain Zeebrugge at Port of Antwerp-Bruges

A modern port is not only a logistics hub, but also a dedicated high-security zone where every risk must be detected early. That is why Belgian ports are investing in an extensive detection network that combines land, water and air. From an advanced radar network to smart cameras and drones, technology acts as the eyes and ears of the port area.

Centralised monitoring from control rooms

Vessel Traffic Centre

The Vessel Traffic Centre is the backbone of maritime surveillance. It is a centralised control room overseeing shipping traffic. Through extensive radar and camera systems, Vessel Traffic Services (VTS) continuously monitors shipping in and around the port zones. In Antwerp, this is based at the Antwerp Coordination Centre (ACC).

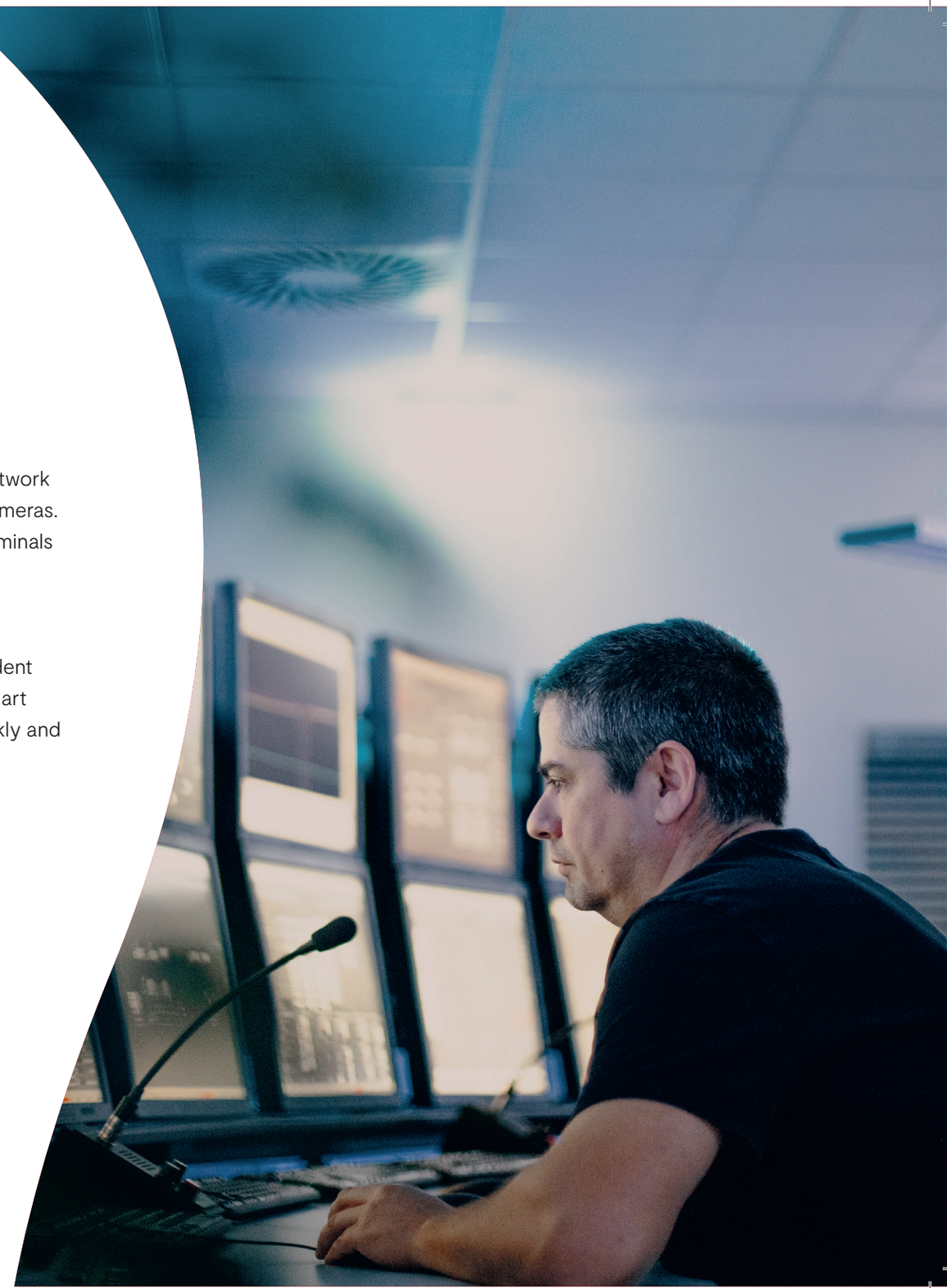
Central Control Room

The Central Control Room (CCR) was set up in Zeebrugge. The CCR improves communication, safety and security of operations at the port. Hundreds of cameras from the security services of private companies connect to the control room, where all these images are monitored.

AI-powered camera networks

At Antwerp terminals and in North Sea Port, there is an extensive network of fixed and mobile ANPR (Automatic Number Plate Recognition) cameras. These systems record vehicle number plates at gates, roads and terminals and automatically link them to access rights or risk profiles.

In addition, smart cameras with artificial intelligence keep an eye on Antwerp and Zeebrugge. The cameras recognise ships, provide incident follow-up support and can be shared with security services. The smart cameras detect individuals and problems in the traffic network quickly and easily, and immediately alert the central control room.



Drones

Airspace is becoming increasingly important in detection. A permanent drone network is active in Antwerp to support aerial inspections, observations and emergency interventions. North Sea Port also deploys drones for inspections, with additional drone detection under development to intercept unwanted aircraft in good time.
There is also a 'drone in the box' on the roof of Port of Limburg. Local police use it in incidents in the Genk-Zuid area, where most of Limburg's port facilities are located.

Zeebrugge is home to a drone detection platform, which the Central Control Room uses to monitor the airspace 24/7. In so doing, they take into account external threats such as climate activism, any NATO or non-NATO military ships nearby, etc.

Mobiele scanners

Finally, the mobile container scanners of customs are strengthening the detection arsenal. This equipment ensures the fast, local and targeted inspection of goods without major logistical delays. The scanners avoid having to move the container, under escort, to a Border Inspection Post, thereby providing a more efficient and faster scanning procedure.

Patrol vessels

On the water, both the Waterway Police and the port companies ensure a visible presence through modern patrol vessels. The Waterway Police recently commissioned new vessels that they are deploying both in the ports and waterways to the ports.

The Waterway Police in Ghent now has a patrol vessel for the port area and a rapid intervention vessel. The Port of Antwerp-Bruges also commissioned two new enforcement vessels in 2022. In the port of Antwerp, the Waterway Police can deploy two patrol vessels and a rapid intervention vessel. With the establishment of a post of the waterway police in Limburg in 2023, a new patrol vessel was also commissioned in 2024.

Port security

Given the national importance of the port of Antwerp, the Waterway Police deploys a specific port security team in addition to the regular intervention teams. They secure the port as a vital infrastructure against terrorist and criminal organisations.

Other security projects

In addition to physical surveillance and access control, Belgian ports are also investing in innovative systems that strengthen security in every link of the logistics chain, both at the terminal itself and in the digital environment.

Certified Pick-Up: control all the way to the container door

With Certified Pick-Up, Port of Antwerp-Bruges introduced a fully digital and secure container release mechanism. Where previously paper documents or PINs were used, the system now works through an integrated, identity-based authorisation chain. Only the correctly registered transporter will have access to the container at the time of pickup.

The result: less fraud, less misuse of PINs and full traceability of every transfer. After one year, more than one million containers had already been released through this system – a clear indication of the broad acceptance within the industry.

Port of Limburg has also ensured a secure container collection process with the T-Mining Secured Container Release system, linked to ItsMe®.

Digital Twins: the virtual view of reality

To respond more quickly and accurately to incidents, ports are building Digital Twin platforms (such as APICA at Port of Antwerp-Bruges). These digital twins of the port area combine real-time data from sensors, cameras, traffic systems and weather information.

They give operators a ‘third eye’ on the ground, allowing them to monitor and simulate both daily operations and emergency situations more efficiently. Digital Twins are therefore becoming strategic tools for incident detection, planning and risk analysis.

Cyber resilience

Digital resilience is as essential as physical security. That is why several ports are rolling out cyber resilience programmes.

Port of Antwerp-Bruges has a specialised cyber team that works according to the three lines of defence model: operational monitoring, expertise & advice, and internal audits. Active identity verification, automated access management and asset monitoring through platforms such as Armis make unauthorised devices or connections immediately visible. However, prevention remains crucial: through awareness programmes, all Port Authority Antwerp-Bruges staff are prepared for possible incidents.

North Sea Port is working with other Dutch seaports on a national cybersecurity platform, under the coordination of government and security services. By sharing knowledge, joint threat analysis and training, companies in the port chain are made more resilient.

Initiatives such as the “Cyber Resilience in the Port” inspiration session by Alfaport Voka show how awareness and collaboration are crucial in making the digital line of defence as strong as the physical one.

Port 2 Port

Security Platform