Council of the
European Union

Brussels, 4 May 2023
(OR. en)

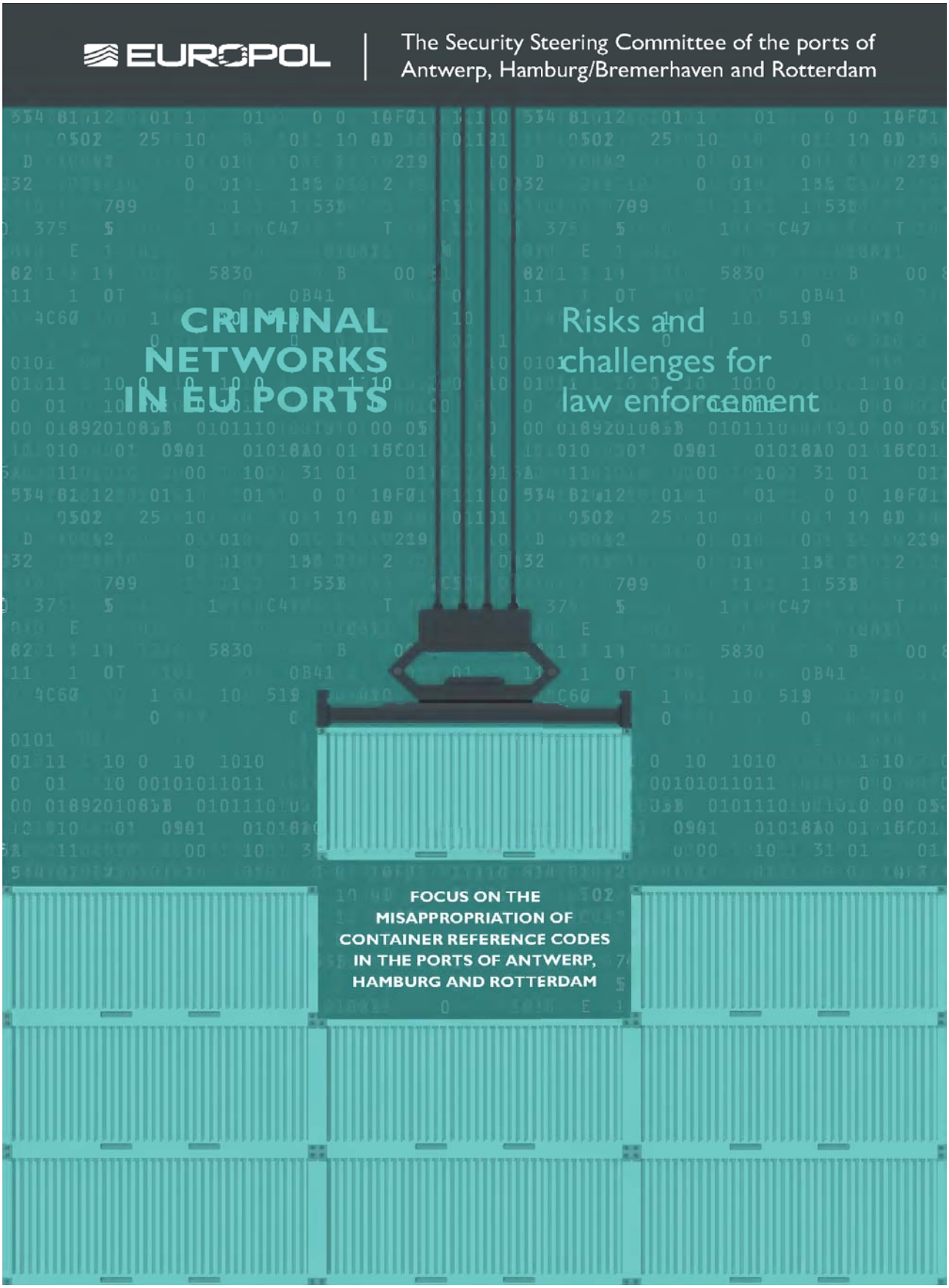
8873/23

COSI 79
ENFOPOL 220
CRIMORG 70
CT 83
CORDROGUE 45
ENFOCUSTOM 52
JAI 556

NOTE

From:	Europol
To:	Delegations
Subject:	Criminal networks in EU ports - Risks and challenges for law enforcement

Delegations will find in the annex the joint report of Europol and the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam "Criminal Networks in EU Ports - Risks and challenges for law enforcement".



Joint report of Europol and the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam

Public document

Date: 30 March 2023

CONTENTS

KEY POINTS

- EU ports are critical infrastructure that facilitate the transportation of goods across the continent and ensure a smooth functioning of the European market. While the vast majority of the trade run through EU ports is legitimate, ports are also exploited for moving shipments of illegal goods into the EU and are vulnerable to infiltration by criminal networks.
  The sheer volume of containers (over 90 million) handled each year, and the low percentage (between 2 and 10 %) that can be physically inspected, makes detection of illicit goods extremely challenging.
  With many public and private actors having access to port infrastructure and port information, opportunities for infiltration and facilitation of illicit shipments are manifold.
- Criminal networks arrange the infiltration of ports and coordinate local networks of corrupted port insiders to organise the passage of containers containing illicit goods into the EU. For this, they rely on worldwide networks of cells with trusted members, or use dedicated service providers. They work in a targeted way, by analysing insider data to select container shipments that are less likely to be inspected and that are organised by logistics companies where they have access to corrupted actors.
- Among the various methods to extract illicit goods from ports, the use of misappropriated container reference codes (or so-called PIN code fraud) has gained traction among criminal networks in recent times. This modus operandi (MO) has mainly been detected in the container ports of Antwerp and Rotterdam, and allows for inconspicuous criminal operations. It is estimated that at least 200 tonnes of cocaine have been trafficked through these ports using this MO in the last years. Relying largely on two factors – a corrupted logistics company employee to provide the reference code and a driver to pick up the container with the reference code – there is no need for physical presence within the port area.
- The MO of misappropriation of container reference codes reflects how criminal networks continuously look for loopholes in port procedures and gaps in security.
  One of the most effective measures to close loopholes/gaps in the logistics process is the principle of access to data and data systems on a need-to-know basis. Logistics companies limiting access to container reference codes has already proven to be an effective solution against this MO. Other preventive measures to be taken by ports and port related actors include logging and traceability of database access to sensitive data, warning systems to detect irregularities, and increased checks of truck driver credentials at the terminals to strengthen container release procedures.

- Closing one loophole will likely steer criminal networks to other opportunities. Besides shifts to other MO for extraction, criminal networks may divert their operations to secondary EU ports with less stringent security measures in place. The development of the EU project to link 328 ports, including secondary ports, to the comprehensive Trans-European Transport Network by 2030 could reinforce this trend.

- Corruption is the key enabler for criminal infiltration of ports. The logistical processes carried out in ports entail participation from various actors that can be targeted for corruption, all providing targets for corruption. This includes port workers and personnel of shipping companies, freight forwarders/shipping agents, importers, transport companies, terminals, security companies, law enforcement and customs. Bribery fees may reach hundreds of thousands of euros. The highest fees are paid to essential links in the extraction chain, often crane operators, planners or employees providing access to information via IT systems. Coordinators of extraction teams receive between 7 to 15 % of the value of the illicit load.

- As a side effect of the criminal operations in ports and the rivalry it entails, violence often spills out of major transportation hubs onto the streets of surrounding cities, where competition for distribution takes place. This has already resulted in the victimisation of innocent bystanders.

- International information exchange on the criminal networks' activities in ports with Europol and amongst EU Member States should be further enhanced. To combat criminal networks in the international context in which they operate – and tackle the high value targets behind them – timely international information exchange is indispensable.

- An adequate response against the misappropriation of container reference codes and other MO for extraction of drugs requires a Europe-wide approach, including a common approach to port security, and closer cooperation with private partners. Public-private partnerships can be platforms where port authorities, law enforcement and justice agencies, and private companies involved in port- related activities, come together. These partnerships can offer the opportunity to exchange tactical and operational intelligence, identify vulnerabilities in port procedures on a European level, and promote and implement security measures to close the loopholes.

BACKGROUND

In 2018, law enforcement authorities of the port of Rotterdam detected a new MO used by criminals networks involved in trafficking of illicit goods: the misappropriation of container reference codes. The port of Antwerp was also affected. Based on analysis, Antwerp and Rotterdam port authorities estimate that hundreds of tonnes of drugs have been trafficked through their ports using this MO.

To tackle this problem and enhance the EU approach to the trafficking of illicit goods in ports, the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam, together with Europol agreed to draft a joint analysis report assessing the threat of infiltration of port infrastructure by organised crime in the EU.

This joint analysis describes and assesses criminal networks' infiltration in EU ports in general, as well as their activities and their modi operandi – including how they use vulnerabilities in port security and maritime shipping procedures to organise the trafficking of illicit goods. The report highlights drug trafficking using containers and the MO for extraction of the illicit goods from the ports. The focus is on the situation in the ports of Antwerp, Hamburg and Rotterdam, where the MO of misappropriation of container reference codes (so-called PIN code fraud) illustrates how criminal networks exploit the loopholes in port and logistic procedures.

The ultimate objectives of this report are to raise awareness among private and public authorities, to encourage EU-wide information exchange, and to provide recommendations to develop a European approach.

This report is based on analysis of the strategic and operational information from law enforcement authorities participating in the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam. It is also informed by the information collected throughout EU Member States' investigations and the findings of the EU Serious and Organised Crime Threat Assessment (EU SOCTA) 2021. This is complemented with information from recent Europol reports, from EU Member States and Europol Third Partners, and open sources.

Misappropriation of container reference codes, also called PIN code fraud

When a container is shipped overseas, the shipping company assigns a unique container reference code (PIN code, QR code, or other unique identifier) to each container after receiving payment for the transport. The code is used to confirm that the container can be released in the destination port and the client can pick up their container. Using mainly corruption, criminals infiltrate the companies involved in the logistics process and obtain the container reference code of the container where they know the ordered drugs are concealed. With the reference code allowing the release, the criminals retrieve the drugs container from the port terminal pretending to be the legitimate client. Once outside the port area, the drugs are extracted from the container. *(See chapter 'Taking advantage of vulnerabilities in the logistics chain').*

THE INFILTRATION OF EU PORT INFRASTRUCTURE BY ORGANISED CRIME

Ports are key for the functioning of the European market and facilitate the transit of a high volume of legitimate movements of goods from across the world. Due to their nature however, ports are also targeted by criminal actors to orchestrate the movement of illicit goods, driving criminality within the ports as well as in their hinterland. Criminal networks particularly rely on maritime transport for high-volume trafficking. Ports are key locations for criminal networks, incentivising them to invest heavily in the infiltration of these hubs. Cocaine, heroin, (pre-)precursors, essential chemicals for synthetic drugs, cannabis (herbal cannabis and cannabis resin), and illicit tobacco products enter the EU in large quantities through ports. Synthetic drugs produced in the EU, counterfeited goods, illicit waste, and stolen vehicles or vehicle parts are shipped throughout the world departing from EU ports. Using the vulnerabilities of ports, criminal networks become structurally embedded in the port environment, legal trade, infrastructure, and facilities.

Vulnerability of EU ports for infiltration

Seaports are spaces with unique geographic and spatial qualities. By their nature, they are vulnerable to criminal threats due to multiple factors, such as:

- their open structures,
- the need for accessibility,
- the vast volumes of shipments they process,
- automation,
- ports' connectivity with the surrounding areas and further transport links,
- the large numbers of companies and personnel on the scene.[1]

The volume of goods handled 24/7 and the size of a port are important determinants for the level of vulnerability for trafficking of illicit goods, and therefore the risks for infiltration by criminal networks. EU ports handle an immense volume of goods. The total gross weight of goods processed in the main EU ports[2], making

1 Lantsman, L., *Seaport Vulnerability to Criminal Networks: A Mixed Method Approach to Measuring Criminological Vulnerability in the Top 30 U.S. Container Ports*, accessed via https://academicworks.cuny.edu/gc_etds/2009/, The Graduate Center, City University of New York, 2017, p. 32.

2 A main port is a statistical port which has annual movements of no less than 200 000 passengers or recording more than one millions tonnes of cargo. For ports selected on the basis of only one of these cargo or passenger criteria, detailed statistics are required only for that transport.

up the legal trade, was estimated at 3.5 billion tonnes in 2021.[3] Containerised goods accounted for 25 % of the goods handled in these ports corresponding to 98 million containers (twenty-foot equivalent unit – TEU).[4] The 20 largest cargo ports[5] handled almost 80 % of all the containers processed in EU main ports in 2020. Rotterdam was the EU's largest container port in 2020 (13.4 million TEU), followed by Antwerp (12.0 million TEU) and Hamburg (8.8 million TEU).[6]

The percentage of containers inspected is low: only approximately 10 % of the containers originating from South-American countries[7] and 2 %[8] overall. Although the number of seizures has increased, the likelihood of containers with illicit goods being detected remains low, especially given the high levels of traffic and daily container throughput.

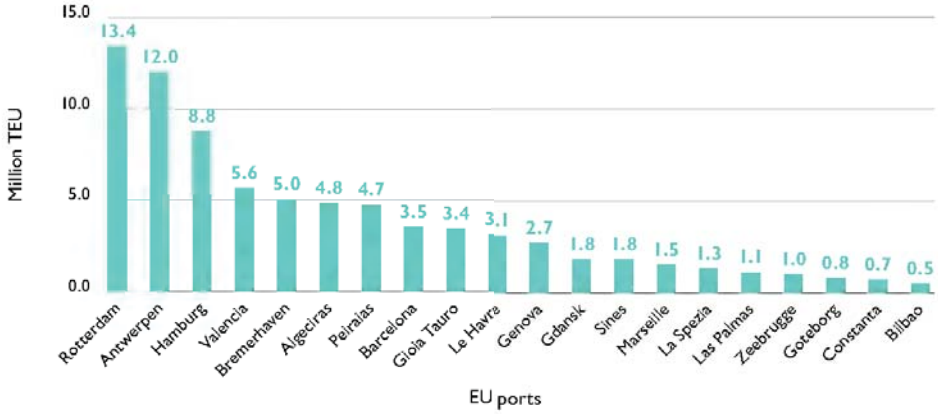


Figure 1: Top 20 EU port - volume in (in million TEUs) of containers handled in 2021
(source: Eurostat - table: mar_mg_am_pvh, 15/11/2022)

In order to achieve high efficiency in port operations, automation is increasing. A high level of automation also creates a new set of vulnerabilities for data breaches[9], unless mitigated with strong cybersecurity measures and internal security procedures.

3 Eurostat, *Maritime freight and vessels statistics – Statistics explained*, accessed via https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Maritime_freight_and_vessels_statistics, 2022.

4 Twenty-foot equivalent unit, abbreviated as TEU, is a unit of volume used in maritime and rail transport statistics, equivalent to a 20-foot ISO container.

5 Rotterdam (NL), Antwerpen (BE), Hamburg (DE), Amsterdam (NL), Algeciras (ES), Marseille (FR), Valencia (ES) Trieste (IT), Pireaus (GR), Le Havre (FR), Barcelona (ES), Bremerhaven (DE), Genova (IT), Klaipeda (LT), Gdansk (PL), Constanta (RO), Sines (PT), Göteborg (SE), Dunkerque (FR), Zeeland Seaport (NL).

6 Eurostat, *Maritime freight and vessels statistics, calculation based on data from tables Eurostat(mar_mg_am_pvh) and Eurostat(mar_mg_am_cvh)*, accessed via https://ec.europa.eu/eurostat/databrowser/explore/all/transp?lang=en&subtheme=mar&display=list&sort=category&extractionId=MAR_MP_AA_PPHD, 2022.

7 Europol, report of meeting with Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam, The Hague, 25/01/2023.

8 EU Commission – EU Science Hub, *Monitoring container traffic and analysing risk*, accessed via https://joint-research-centre.ec.europa.eu/scientific-activities-z/monitoring-container-traffic-and-analysing-risk_en, date accessed: 2022

9 Lantsman, L., *Seaport Vulnerability to Criminal Networks: A Mixed Method Approach to Measuring Criminological Vulnerability in the Top 30 U.S. Container Ports*, accessed via https://academicworks.cuny.edu/gc_etds/2009/, The Graduate Center, City University of New York, 2017, p. 41.

Criminal networks are interested in operating "a safe trade, regardless of the economic costs".[10] The safety of trade depends on the criminal network's ability to successfully avoid customs and police controls. Therefore ports are also selected based on the possibilities to infiltrate and control port logistics and transport services. The high numbers of service providers and companies with access to the port area, alongside the presence of many peripheral port companies (such as freight forwarders and cargo handlers) offers ample criminal opportunities. They enable port infiltration, corruption, setting-up of front companies, and sending illicit cargo within the legitimate stream of commerce to circumvent customs controls.

Large networks organising overseas trafficking of drugs to the EU

International criminal networks rely on locally-embedded coordinators and their accomplices to corrupt port personnel and organise the passage of the illicit goods through ports. If criminal networks are not able to (or choose not to) set up the port infiltration themselves, they make use of local criminal networks who have already infiltrated the ports and are offering their services. Over time, criminal networks have, either directly or indirectly, established footholds in many EU ports. Some criminal networks have a long history in certain ports, operating there for more than a decade.[11]

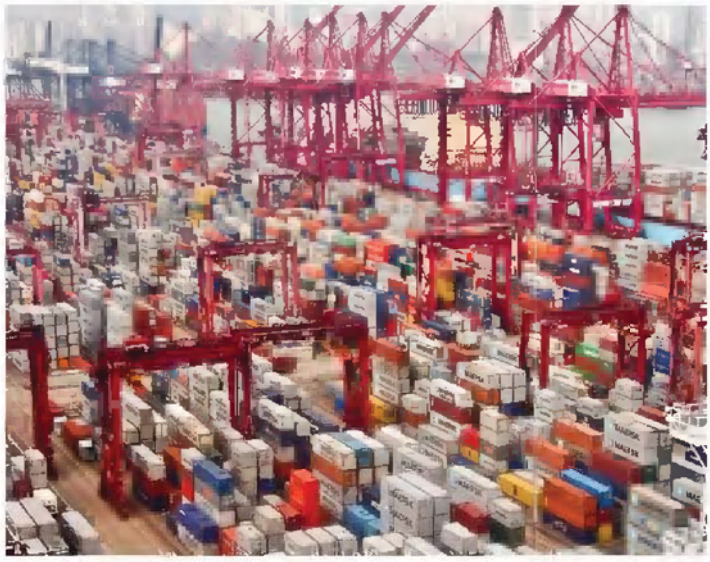
Larger integrated criminal networks are able to oversee the whole overseas drugs trafficking chain from supply to distribution by establishing cell and branches with trusted members in different territories. These networks arrange and coordinate the acquisition of the drugs, the infiltration of the ports to introduce and extract the goods, the transport logistics, the supervision of the shipments, and the final distribution. Alternatively to the end-to-end business model described above, drugs also reach the EU through interconnected networks of independent suppliers, transporters, brokers, extractors and EU-wholesale and retail distributors working together with each partner focusing on a specific part of the trafficking process. In most cases, the business model of criminal networks falls somewhere between these end-to-end and independent collaboration models.

10 Antonelli, M., *An exploration of organized crime in Italian ports from an institutional perspective. Presence and activities*, accessed via https://link.springer.com/article/10.1007/s12117-020-09400-z, Trends in Organised Crime Vol. 24, Springer-Verlag, 2021, p. 152–170.

11 Antonelli, M., *An exploration of organized crime in Italian ports from an institutional perspective. Presence and activities*, accessed via https://link.springer.com/article/10.1007/s12117-020-09400-z, Trends in Organised Crime Vol. 24, Springer-Verlag, 2021, p. 152–170.

EXTRACTION OF ILLICIT GOODS TRAFFICKED WITH MARITIME CONTAINERS

A variety of modi operandi are used to organise overseas maritime trafficking of drugs. Criminal networks can opt to hide the illicit goods in the ship itself, attached to the outer hull or hidden in containers loaded on the ship. Illicit goods can either be retrieved before ships reach the port or after their arrival. Transport vessels include roll-on/roll-off ships, cargo vessels, bulk carriers, tankers, reefer ships, cruise ships, sailing boats and yachts, submarines or fishing boats. Pleasure vessels and fishing boats are frequently used to transport large quantities of cocaine and they provide huge flexibility to enter the EU at small marinas and fishing ports. However, the largest amounts found in seizures are hidden in Europe-bound cargo ships, mainly in maritime shipping containers.[12]



When illicit goods are shipped in maritime containers, criminals use a variety of means to obscure the cargo. It may be hidden in (sport) bags and placed in an easily accessible place in the container, concealed in the legitimate goods (e.g. hidden between boxes of fruit), physically incorporated in marble blocks, chemically incorporated in textiles or coal, or hidden in the construction elements of the container such as roof, floor, back wall or cooling elements.

Once the illicit goods arrive in the destination port, the goods can be extracted **from the container in the port** by an extraction team who leave the port area on foot or in a vehicle, or the goods **leave the port in a container** and are collected **outside the port area**.

In order to ensure 'safe' transit of the illicit goods in containers, criminal networks will analyse data obtained by insiders. With this information, they target those shipments that are going to the desired destination, are less likely to be inspected, and that are organised by logistics companies where they have access to corrupted actors. These are referred to by criminals as 'green lines'.

12 European Monitoring Centre for Drugs and Drug Addiction and Europol, *EU Drug Market: Cocaine — In-depth analysis*, accessed via https://www.emcdda.europa.eu/publications/eu-drug-markets/cocaine_en, 2022.

Maritime container shipping procedures

In order to understand the MO to extract containers from ports, a more detailed look into maritime container shipping procedures is required. Exporters from abroad, e.g. in South America, sending goods to the EU generally make use of the services of freight forwarders and shipping agents. The freight forwarder or shipping agent contacts the shipping company, organises the transport of the empty container to the exporter to be packed, the transfer to the vessel, the port paperwork (including transport insurance), the customs checks, the payment of port services and the final inspection of the container on behalf of the exporter. It is also the freight forwarder or shipping agent who will collect the bill of lading[13] from the shipping company and send it to the importer in the EU.

In the next step, the container is loaded onto the vessel and shipped to its destination. Before the vessel arrives in the destination port, the shipping company creates a unique reference code, the so-called PIN, for each container. Container reference codes are often provided in the form of a PIN code, but can also be QR codes or other unique identifier codes. With the container reference code the importer, his representative, or transporter can pick up the container from the destination terminal. The code is only sent to the importer after the shipping company has received the payment for the transport. At that time, the terminal where the container will arrive in the destination port receives the reference code as well.

When the ship reaches the destination port, the container is unloaded and transferred to a terminal. The location of the container in the terminal depends on its destination and origin (EU or non-EU) and the subsequent mode of transportation (sea, railway, road, inland waterways). The container number, which is stored in the port's data systems and linked to a specific stack position, is used to establish the exact location of a container in a terminal, while the PIN code is used for retrieving the container.

Four main types of containers can be found on the terminal area:

- containers just arriving, awaiting to be moved to a more permanent location;
- containers in transhipment to another destination in or outside the EU;
- containers in transit within the EU;
- containers from outside the EU to be imported into the EU.

13 Cambridge dictionary: bill of lading is a document that shows the details of the products that are being transported by a company. With the bill of lading, the carrier acknowledges that it has received the goods that are to be transported. The buyer must present the bill of bading in order that the goods can be released, (https://dictionary.cambridge.org/dictionary/english/bill-of-lading).

These containers may be allocated to a specific physical location within a terminal. However, in more automated ports, containers are mixed together and placed in function of minimising stack movements. So, for example, a transhipment container can be found next to an intra-EU container or an empty container.

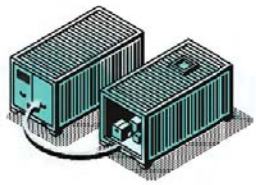
After the arrival of a container destined for import in the EU, a representative of the importer (often a freight forwarder) will present the bill of lading and other documents to customs, mostly via a digital platform. Customs will check the documents and decide on the next step: an immediate release (most of the containers), a thorough check of the customs declaration and the bill of lading, or a physical check of the container, which includes a scan and is sometimes complemented with the opening of the container.

Once customs agrees to release a container and other formalities with port and shipping company are resolved, the custody is transferred to the representative of the importer. The importer provides the container reference code and other relevant documents to the transport company that sends a truck driver to pick up the container. The terminal verifies the container reference code and credentials presented by the truck driver and releases the container. Once the content of the container is unloaded by the importer, the empty container is returned to the shipping yard.[14]

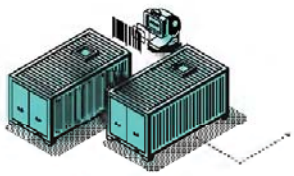
14 Wankhede, A., Watch: *How Container Shipping Works – The Process Of Transporting Cargo in Containers*, accessed via https://www.marineinsight.com/videos/watch-how-container-shipping-works-the-process-of-transporting-cargo-in-containers/, Marine Insight, 2021.

Modi operandi for extraction of drugs from containers

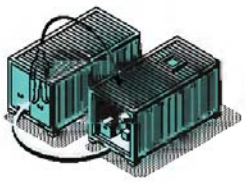
In maritime container drug trafficking, the **rip-on/rip-off method** is one of the main MO employed by traffickers. In the port of departure, the drugs are placed in the container in a place which is easily accessible. The drugs are then transported along with the goods from a legitimate receiver/importer, who is often unaware of the situation. At the destination, the drugs are retrieved in or outside the port by extraction teams.



The newer **switch method** has been increasingly observed over recent years. This MO involves the transfer of drugs from a non-EU container to another container which has less or no risk of being controlled. Often the drugs are transferred to a container in intercommunity transport from one EU country to another as these containers are seldom inspected. Alternatively also empty, transhipment or export containers are used.



Another variation of the switch method is the **cloning** of containers. This method involves a container scheduled for a scan and control by customs. When the container is transported to the scanner, the original container leaves the port area and is replaced by a replica container (clone) with the same registration number as the original container.



All of these modi operandi require the support of insiders operating in the port. The insiders include corrupted port personnel but also extraction teams brought into the port with a '**Trojan horse container**'. These are often export containers with an extraction team inside which are transported into the secure port area, sometimes days before the arrival of the illicit goods.

Because of the complex process of tracking the arrival of containers and their movement within ports, and the need for insider support, each entry point of illicit goods can be considered a hotspot for corruption. For most MO, the major challenge is determining the stack position, which is the location of the container on the terminal between the thousands of other containers. Containers can be stacked in blocks with containers placed in the interior of the block or very high up, making them difficult or impossible to access. To locate and ensure accessibility, collaboration of multiple corrupted dock workers, container drivers and crane operators is almost always necessary.

However, the increasing digitalisation of port infrastructures offers other opportunities for extractors and is reflected by the rising number of incidents involving breached and manipulated IT systems. An illustration of this evolution is the misappropriation of container reference codes which have been recovered from data systems of actors involved in the logistics chain. This MO particularly affects the port of Antwerp, Hamburg and Rotterdam. One of the major advantages of this MO is that it does not require the support of insiders in the port area to extract the illicit goods.

MISAPPROPRIATION OF CONTAINER REFERENCE CODES IN THE PORTS OF ANTWERP, HAMBURG AND ROTTERDAM

Being the largest container ports in the EU, Antwerp, Hamburg and Rotterdam are severely affected by maritime drug trafficking using containers. Criminal networks target these ports mostly because of the possibility to hide drugs among the enormous inflow of containers and the many actors with access to the port who provide opportunities for infiltration. As part of the Trans-European Transport Network (TEN-T)[15], interconnecting maritime, rail, road infrastructure as well as inland waterways, the highly-automated ports of Antwerp, Hamburg and Rotterdam are perfect hubs for criminal networks. Being well-connected to the European transport system, an efficient EU-wide distribution of drug consignments can be organised from these ports.

Taking advantage of vulnerabilities in the logistics chain

In 2018, law enforcement authorities of the port of Rotterdam increasingly received reports of containers being stolen, disappearing, delivered at wrong addresses or found in unexpected locations. Criminal networks had detected a vulnerability in the logistics chain, allowing them to illegally retrieve container reference codes, which are required to pick up containers in the ports. This enabled them to circumvent container release procedures and illegally transport containers with illicit goods outside port area. The ports of Antwerp and Hamburg were also concerned.

The basic principle of the MO of misappropriation of container reference codes is simple. As mentioned in the chapter on maritime container shipping procedures, a shipping company produces the unique container reference code (PIN, QR, other unique identifier) for each container once the transport has been paid. With this code, the shipping company confirms that the container can be released in the destination port and the client can pick the container up from the terminal in the destination port. The code is transferred to the importer or the freight forwarder working on behalf of the importer, and by the freight forwarder/importer to the transport company picking up the container at the destination. The code is also sent to the terminal where the goods will arrive in the destination port, so that the terminal can check if the correct container reference is provided by the transporter and

15 European Commission, *Ports 2030 – Gateways for the Trans-European Transport Network*, accessed via https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/brochures_images/ports2013_brochure_lowres.pdf, 2013.

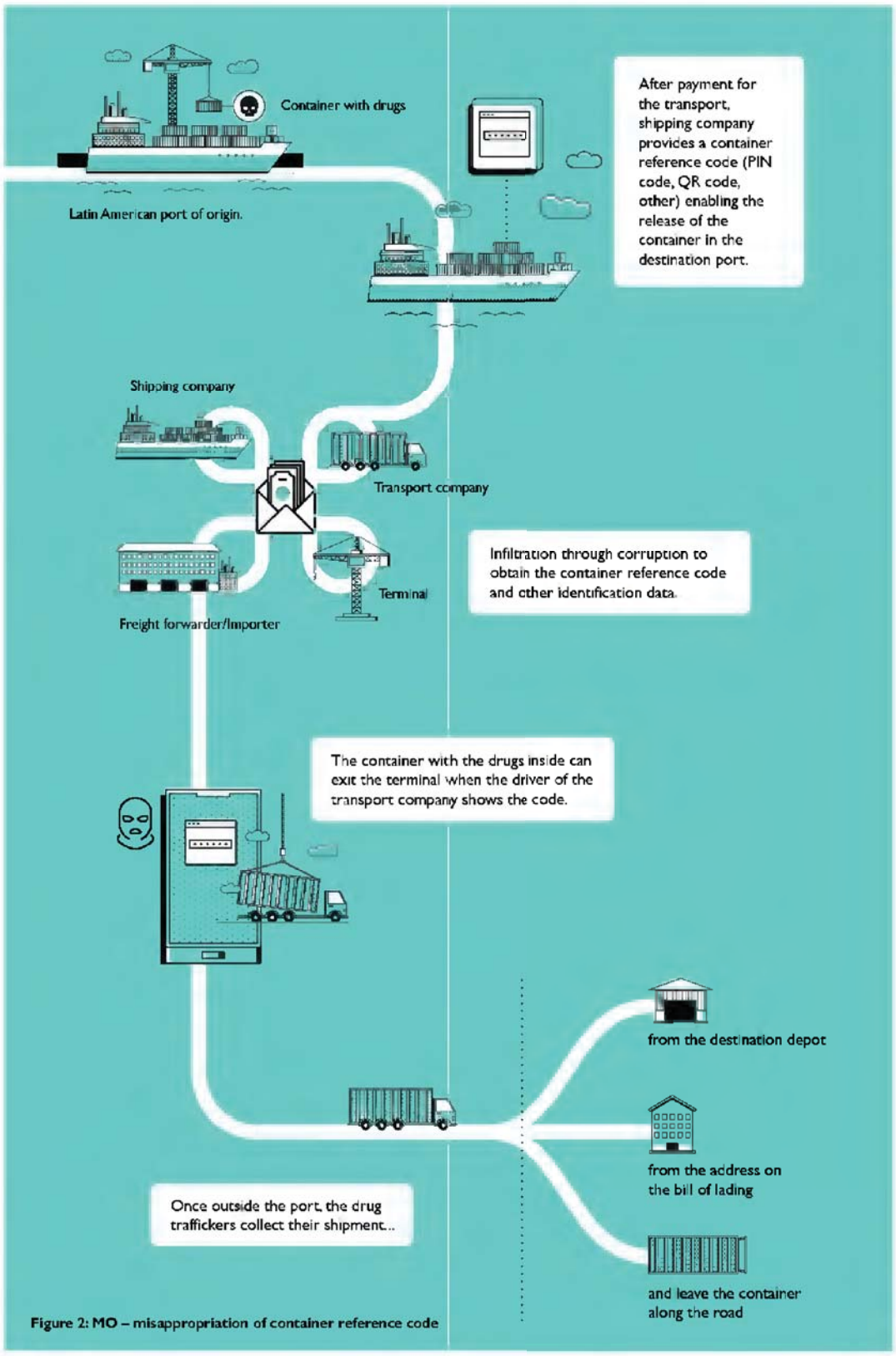


Figure 2: MO – misappropriation of container reference code

the container can be released. Using mainly corruption, criminals infiltrate the companies involved in the logistics process and procure the reference codes of the containers where their drugs are concealed, preferably without the knowledge of the lawful owner. The codes are provided to the driver of a transport company working for the criminal network, who retrieves the containers from the port terminal while pretending to be the legitimate client. Outside the port, the drugs are extracted from the container. Afterwards, some criminal networks will try to deliver the container to the rightful owner. In other cases, containers are just left along the road or made to disappear.

Criminal networks mostly receive the codes from corrupt individuals who unlawfully use the accounts of legitimate companies involved in transport and port logistics. In some cases however, they may deploy hacking or phishing. Once the criminals have the container number and the container reference code, they can gain access to detailed information about the status of the container as it is logged in the integrated and automated port data systems. They can also check if the container is present and ready for release, in order to schedule an illicit pick-up.

The misappropriation of container reference code is an MO seen both in automated and non-automated terminals. In automated terminals where traditional MO building on a network of corrupted connections in the port sometimes becomes more difficult, this method offers an excellent alternative.

Multiple possibilities to organise the infiltration

The MO of misappropriation of container reference codes presents several advantages for criminal networks. It reduces the required number of corrupted individuals inside the port to a minimum as the container is brought to the truck; this means that container movements inside the port are irrelevant for the retrieval. Basically, all that is needed is a corrupted employee providing the reference code and a truck driver working for a corrupted transporter.

In addition, as several stakeholders are involved in the transport process, criminal networks have multiple options for targets that can be approached for corruption. The importing company, the shipping company, the terminal of arrival or transit, the transport companies, the freight forwarders and shipping agents, all provide infiltration opportunities, as they all have (at some point in the process) access to the reference code. This is particularly true when reference codes and other information concerning the container are not in well-protected data systems and many employees have access to it. Some large logistics companies have one information system connected worldwide, allowing access

to sometimes thousands of individuals. Without strong internal security procedures, criminals can easily find suitable targets to bribe and to retrieve the necessary information to set up the theft or diversion of the container.

In order to counter the threat of misappropriation of container reference codes, the port of Rotterdam started a pilot project with the private sector. Prompted by assessments of the Dutch law enforcement authorities active in the port of Rotterdam, a shipping company implemented a security system limiting the number of individuals with access to the references codes. This simple measure had an immediate effect and the number of the cases of misappropriation of container reference codes drastically dropped. This pilot showed that although economic considerations can form a hurdle for private companies stepping into these prevention projects, they are willing to step into public-private partnerships and be an essential part of countering this threat.

Undetected in other EU ports due to underreporting?

At the moment, Europol has no information on the use of the MO of misappropriation of container reference codes or similar MO in other EU ports. However, criminal networks undoubtedly also look for vulnerabilities in these other ports to circumvent container release procedures. Law enforcement authorities in Antwerp and Rotterdam presume a substantial underreporting of this MO. Because of the underreporting, the threat of misappropriation of container reference codes or similar MO to divert containers with illicit goods could still largely be undetected in other EU ports.

CORRUPTION, THE KEY ENABLER OF INFILTRATION OF PORTS

For criminal actors and criminal networks organising overseas trafficking, access to ports is essential. Corruption is the main enabler to infiltrate ports and logistics chains. Lacking relevant information on container processing and locations, and unable to gain control over port procedures directly, criminal networks – engaging dedicated actors to do so – rely on methods such as social networking and bribery to corrupt personnel active in port or port-related activities. These corrupted personnel facilitate unrestricted access to the ports and port systems for criminal networks.

Building a corruption network

Building on the local coordinators and their accomplices, criminal networks infiltrate ports by corrupting personnel who are:

- directly active in the port such as port workers, terminal operators, security, customs and police;
- employed in logistics companies, in port authorities, semi-public and public authorities with access to port data systems;
- from third party companies with privileged access to the port such as truck drivers or maintenance personnel.

Criminal network members - acting on instructions from the coordinator of trafficking operations - will insert themselves into the community of personnel active in port-related activities. They may do this by gaining access to the social network directly, through sport or leisure activities. They may also take up employment in the port, making contact with port workers on the job and in training sessions. Once the contact has been established, they grow the network of insiders and strengthen the infiltration using corruption and intimidation.

Criminal networks do not just target the personnel of one port. With the support brokers and local coordinators, they will seek to form corruption networks in multiple locations. This practice allows the criminals to be flexible in changing their routes depending on control measures or risks to the shipments. Corrupting multiple workers responsible for a specific stage of the process is also essential, as it allows criminal networks to quickly replace contacts who are taken out by law enforcement, ensuring the continuity of trafficking operations.

The highest bribes for the most crucial actors

The highest bribery fees are logically paid to the most important links in the extraction chain. For example, for the rip-on/rip-off or switch MO, this could be a crane operator placing the container in an accessible location or a planner providing the exact stack position; for misappropriation of container reference codes, it is the employee with access to the code. These fees may be paid with a part of the load or as a percentage of its value. Coordinators of extraction teams receive between 7 to 15 % of the value of the illicit goods. Meanwhile, members of the extraction teams, recruiters of port insiders, truck drivers and employees providing access to IT systems and providing container reference codes are sometimes paid fees ranging in the hundreds of thousands of euros.

The high bribes paid highlight the key role corrupted personnel play. Specialised workers involved in different steps of the physical process, as well as staff of logistics companies, port authorities and customs, have expertise and access to transport and IT infrastructure essential for criminal networks involved in trafficking at ports. Anyone involved at any stage of the logistics process is an asset to criminal networks and, therefore, vulnerable to corruption.

VIOLENCE AS A CONSEQUENCE

Violence is often a side effect of criminal activities carried out in the ports. Violence is used to ensure compliance of corrupted individuals and external facilitators, as well as for fighting out rivalries between criminal networks active in the ports and the settlement of scores. Violence is spilling out of major transportation hubs onto the streets of surrounding cities, where competition for distribution takes place.

Criminal networks use several methods to convince port personnel to cooperate and to remain cooperative. Bribery, often building on a relationship of trust, providing drugs or facilitating sexual services, are part of the arsenal used by criminals to obtain cooperation. When compromised personnel want to step out of a corruption network or, more rarely, criminals need to force unwilling individuals to service them, criminal networks turn to intimidation, blackmail and violence. Furthermore, in an environment of transient networks of brokers, criminal groups and service providers working together, violence also ensures compliance of external criminal collaborators. Violent acts range from threats, intimidation and torture, to murder. Occasionally innocent individuals operating in ports or outside ports are targeted, such as the drivers that legitimately move containers in which drugs may be concealed.

The huge money flows involved in drug trafficking attract numerous criminal actors, all willing to operate in the port area. Although some criminal networks work together in the ports, others engage in extreme violence because of the fierce competition for dominance and profits. The competition between rival criminal networks also entails a trail of subsequent score – settling violence, exposing innocent citizens caught in the middle – as shown in recent clashes between drug traffickers in residential areas of Antwerp.

CONCLUSIONS AND OUTLOOK

The situation in the container ports of Antwerp, Hamburg and Rotterdam, and the MO of misappropriation of container reference codes to extract illicit goods from the ports, clearly illustrate how criminal networks make use of vulnerabilities in the port environment to traffic illicit goods. Using the immense volumes of commodities legally handled on a daily basis and the numerous public and private actors with access to the port and port-related data systems, criminal groups found a convenient way to 'safely' organise their trafficking operations. Highly connected to the European transportation network, these ports offer the opportunity to quickly transport the illicit goods to distribution hubs throughout the EU. If not addressed in an effective and efficient manner, the use of misappropriated container reference codes – and similar innovative MO derived from it – is likely to increase. Criminal networks will continue to use major ports for trafficking and infiltrate them through corruption, as long as loopholes in the logistics chain and security procedures allow.

Many ports are expanding by adding capacity and speeding up processing of containers. With higher levels of automation in ports and increasing digitalisation of cargo handling procedures, adequate mitigation measures need to be put in place both by private and public partners. Major ports are already looking to counter illicit goods trafficking with changes in procedures and developing more secure database systems, and are looking into innovative technologies combining imaging and artificial intelligence to increase the screening rate of containers and goods. As major EU ports increase security, secondary EU ports are likely to become more attractive for criminal networks. Although the volume of containers passing through secondary EU ports is still small compared to the major EU ports, cocaine trafficking through secondary EU ports is increasingly being observed, likely due to less stringent security measures in place. The development of the EU project to link 328 ports to the comprehensive Trans-European Transport Network (TEN-T) by 2030 could reinforce this trend.[16]

With stronger prevention and law enforcement measures in place inside the ports, other displacement effects have to be considered, such as a displacement of criminal network actions to locations outside the ports e.g. violence against legitimate truck drivers unknowingly transporting containers with illicit goods or increased corruption, intimidation and violence against personnel working in import companies.

16 European Commission, *Ports 2030 – Gateways for the Trans-European Transport Network*, accessed via https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/brochures_images/ports2013_brochure_lowres.pdf, 2013.

To combat international criminal networks and the high value targets leading and coordinating their worldwide criminal activities, timely international information exchange of operational, tactical and strategic information is crucial to setup a coordinated approach. Through joint investigations, operational task forces (OTF) and EMPACT, EU law enforcement and justice authorities can take concerted action supported by Europol.

The infiltration of ports by organised crime is a major threat for the legitimate economy and security of the EU. A common Europe-wide approach with attention for regional aspects needs to be implemented in EU ports to tackle this threat, since criminal networks continuously look for loopholes in security, adapt their modi operandi or switch from one port to another seeking more favourable conditions for their operations. This requires strengthening ports' resilience to infiltration, as well as preventive and investigative actions. With the further modernisation and expansion of many EU ports, continuous attention must be paid to the integration of security features in the design of port infrastructure. This includes the development of legislative initiatives at the European level to streamline security measures in ports, as well as implementing public-partnerships to involve all port actors essential for tackling the infiltration of criminal networks in EU ports. Implementation of such measures at the European level will ensure a level playing field, avoiding competition at the cost of security.