Study on corruption vulnerabilities in EU seaports' supply chain

Jasmin Saarijärvi, Gabrielle op 't Hoog, Sabine Hellemons, Federica Genna, Victoria Tokatzian, Halima Guelai, Margarita Gasparinatou, Eirini Stamouli, Júlia Miralles-de-Imperial, Fernando Jiménez-Sánchez

https://doi.org/10.3013/sr700b64

Abstract

This article draws on the results of a study on corruption vulnerabilities in EU seaports' supply chains, developed within the framework of project POSEIDON (PortS unitED Against Corruption). POSEIDON is an EU-funded project (Grant Agreement No 10110337) that seeks to enhance anti-corruption practices in EU seaports. This is done through the mapping and identification of corruption vulnerabilities in the supply chains of EU seaports. Ports and their supply chains are crucial as enablers of trade, but they are also vulnerable to the exploitation of organised crime groups involved in the trafficking of illicit goods such as drugs or firearms. The identification of corruption vulnerabilities and anti-corruption practices is carried out through literature research, interviews, focus groups, surveys and study visits to selected ports in Belgium, Greece, Spain, Italy and the Netherlands. To contribute to EU-level actions against corruption and address vulnerabilities in the port supply chain system, POSEIDON also gathers practices from different public and private stakeholders. The project is still ongoing, but some anti-corruption practices have already been identified, namely digitalisation, training and awareness campaigns, and screening of port employees and staff, along with public–private cooperation. This process of exchange is fostered in the project by a cycle of six thematic dialogues, where different stakeholders from the public and private spheres are brought together to discuss current trends, challenges and good practices in this sector.

The identification and collection of anti-corruption practices is closely connected to the EU public–private network of port sector stakeholders that has been established during the project. The network fosters the exchange of anti-corruption practices and contributes to the mitigation of corruption vulnerabilities in the port sector. The transferability of good practices identified by the project – which will also be displayed via an interactive dashboard

available to the public – will be assessed within the project's life cycle, contributing to the definition of a series of recommendations for an EU port supply chain integrity standard.

Keywords: seaports, corruption, supply chain, vulnerabilities, good practices, port stakeholders, organised crime, infiltration, resilience.

Introduction

This article is a summary of a 2024 study by the POSEIDON Consortium on corruption vulnerabilities in EU seaports' supply chains drafted as part of the EU-funded project POSEIDON ([27]).

The article seeks to identify vulnerabilities for corruption in EU seaports' supply chains. In particular, it aims to contribute to the understanding of vulnerabilities for corruption and, as such, to provide a stepping stone for an improved EU-wide approach against this phenomenon.

The overall objective is to shed light on the vulnerabilities for corruption at different stages of the EU port supply chain. EU seaports are part of the critical infrastructure that enables the transport of goods across Europe (and beyond) and are an essential component of the supply chain that ensures the smooth functioning of the single market (Europol, 2023, p. 4). Corruption in seaports facilitates crime, disrupts trade and undermines the rule of law. As there is no universally agreed definition of corruption, perspectives and interpretations of corruption vary between cultures and countries (European Parliament: Directorate-General for Parliamentary Research Services et al., 2017, p. 5). However, corruption is regularly understood as 'the abuse of (entrusted) power for private gain', a relatively broad concept that covers offences such as active and passive bribery, conflict of interest, clientelism, favouritism and trading in influence (European Parliament: Directorate-General for Parliamentary Research Services et al., 2017, p. 5). The focus of the study at hand is on corruption intended as an 'enabler of organised crime'. While organised crime can exist with and without corruption, the focus of this study lies at the intersection between the two, with its scope delimited to the working mechanisms of EU seaports' supply chains.

Methodology

The research methodology applied includes desk research of over 30 sources at the international, EU and national levels, 12 interviews with public and private actors and 6 case studies (Port of Algeciras, Port of Antwerp-Bruges, Port of Cartagena, Port of Piraeus, Port of Rotterdam and Port of Venice). Additionally, a cycle of six thematic dialogues was organised to gather further input from stakeholders, and a targeted survey was developed and distributed to the law enforcement community across the EU. Further details on each data collection method are presented in the following sections. As outlined above, the scope of the article covers corruption as an enabler of organised crime, with a focus on corruption at the operational level (i.e. in the supply chain). The research has been focused on corruption related to the trafficking of illicit goods from ports located outside the EU into ports in the EU, predominantly through container trade.

([27]) Ports United Against Corruption – Grant Agreement No 101103337 – POSEIDON – ISF-2022-TF1-AG-CORRUPT, POSEIDON, 2023. See: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43252368/101103337/ISF?order=DESC&pageNumber=1&pageSize=10&sortBy=relevance&keywords=poseidon&frameworkProgramme=43252368.

Analytical framework

To facilitate the comprehensive and structured collection of data, an analytical framework was developed, based on a supply chain of legal trade of EU seaports. This draft supply chain was developed based on desk research, scoping interviews and detailed exchanges with the POSEIDON advisory board, supporting partners and relevant port stakeholders and experts on EU seaport supply chains. These activities yielded a comprehensive overview of the different steps in the EU seaport supply chain of legal trade and helped to identify a first set of vulnerabilities linked to these steps, as presented in the figure below.

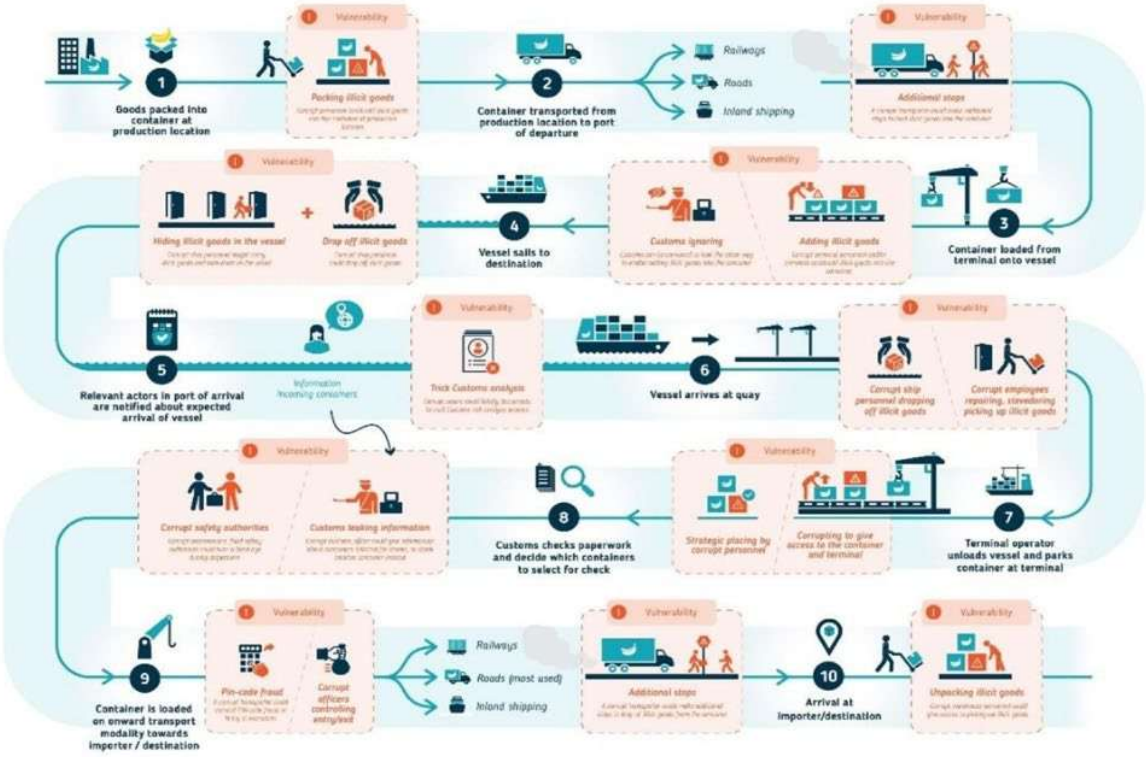

Figure 13.1. Visualisation of corruption vulnerabilities in the port supply chain

Source: POSEIDON.

Data collection

Desk research was conducted taking into account a wide array of documentation. Over 30 documents have been reviewed via desk research, including academic papers, policy documents and reports from (inter)national organisations and law enforcement agencies, at both the international and EU levels. An overview of relevant documentation considered is included in the references ([28]). Moreover, interviews with various seaport authorities, European policymakers and researchers have enriched the study with in-depth insights that complemented findings obtained through desk research.

([28]) This overview does not include the relevant documentation considered in light of the case studies.

Six case studies were conducted in the framework of the POSEIDON project ([29]) with a view to providing seaport-specific insights, illustrating findings with real-world examples. The case studies were selected in such a way to allow for a geographical spread of the seaports across the EU and to ensure a mix between larger and smaller seaports. Each case study involved desk research, interviews with stakeholders, focus groups with economic operators and study visits to seaports.

During the visits (as part of the case studies) to the Port of Antwerp-Bruges, the Port of Algeciras and the Port of Venice, thematic port dialogues were also held ([30]). The purpose of these thematic dialogues was to bring a variety of stakeholders together and to discuss a particular topic related to corruption in seaports with a diverse group of stakeholders. Central topics of the thematic dialogues were public–private cooperation, compliance systems and digitalisation in seaports, and corruption as an enabler of human smuggling.

Lastly, a survey was conducted with a dual objective. Firstly, the survey served as an opportunity to gather information on vulnerabilities for corruption in seaport supply chains outside the six seaports that serve as case studies. Secondly, the survey also provided an opportunity to validate the findings collected through the six case studies. Given the sensitivity of the topic at hand, the survey was only launched within the law enforcement community, within the framework of POSEIDON under the European multidisciplinary platform against criminal threats (Empact) high-risk criminal networks operational action plan (operational action 7.1) ([31]).

Validation of findings

Preliminary findings and conclusions have been verified and validated at several stages, including at a validation session with the POSEIDON advisory board, composed of academics, policymakers and law enforcement representatives, inter alia. Finally, the draft findings and conclusions were presented to the co-leaders and participants of operational action 7.1 of Empact's high-risk criminal network operational action plan, focusing on the prospective impact of these findings on the operational work of the law enforcement community.

Methodological limitations

The research encountered methodological limitations that warrant acknowledgment. First, the selection of seaports for case studies, limited to six, may restrict the generalisability of findings to a broader port context. Limitations in geographical focus are also present due to this, as the case studies only focus on seaports in north-western Europe and southern Europe. This limitation was mitigated by collecting additional data on seaports beyond the selected case study ports through desk research, in-depth interviews, the survey and validation sessions with different types of stakeholders. Second, distinguishing between organised crime and corruption posed a significant challenge. The intertwined nature of these phenomena, often due to blurred distinctions, complicates the assessment of individual contributions to corrupt practices within seaport environments. Due to the sensitivities surrounding corruption in countries, the tendency to apportion blame to organised crime instead of corruption emerged as a difficulty. These

([29]) Case studies have been implemented as follows: Port of Piraeus (September 2023), Port of Antwerp-Bruges (November 2023), Port of Algeciras (January 2024), Port of Rotterdam (February 2024), Port of Cartagena (March 2024), Port of Venice (April 2024).

([30]) The organisation of thematic dialogues is part of Poseidon's work package 4, and contributes to fostering inter-port exchanges and dialogues, supporting the establishment of a public–private port stakeholder network.

([31]) Poseidon serves as inspiration and driver for Empact's fight against high-risk criminal networks (operational action 7.1), which formally kicked off in February 2024.

limitations highlight the need for a cautious interpretation of findings and suggest ways in which this can be addressed in future research more comprehensively.

Key findings

The research has yielded many relevant and concrete insights into corruption vulnerabilities in the different ports in the case studies. Whereas the vulnerabilities for corruption in the supply chain tend to be relatively clearly demarcated, the more structural features in and around ports that increase vulnerability to corruption are less tangible, more complex and, likely, more difficult to address. Some of these vulnerabilities directly affect the possibility of corruption risks, while others have a more indirect effect on corruption risks.

This section first describes the vulnerabilities with a direct impact (i.e. types and origin of goods, the involvement of people, social communities around the port and the role of politics) before addressing the more indirect factors (i.e. the economic climate in the port, the type, size and location of the port, the cooperation between actors in the port, and legislation). Subsequently, the corruption vulnerabilities in each step of the port supply chain are highlighted.

Vulnerabilities related to corruption in seaports

Types and origin of goods and shipments

The ports examined in this article suggest that certain types of goods, modalities and trade routes pose more vulnerabilities related to corruption than others. Regarding the types of goods, perishable goods are particularly vulnerable (Europol, 2023; GI-TOC et al., 2021, p. 42; Roks et al., 2021, pp. 182–184; EMCDDA et al., 2019, p. 7) and are used to conceal different kinds of illicit goods such as drugs, illegal waste and counterfeit products. The limited scope for inspections of these shipments creates a vulnerability that can be exploited by corrupt personnel including both public authorities and/or private actors in the seaport (e.g. customs authorities, ship agents and freight forwarders) ([32]), as they can purposefully overlook parts of a container or shipment during the check and/or refrain from reporting suspicious items ([33]). Various types of shipments can be vulnerable to corruption, with container trade being among the most frequently mentioned (EMCDDA et al., 2022, p. 24; Roks et al., 2020, pp. 182–183; GI-TOC et al., 2021, pp. 38–40). Containers are attractive for illicit activities, inter alia, due to their size, limited visibility of their contents and the high volume of their throughput ([34]). The nature of trade routes connected to a seaport also impacts the corruption vulnerabilities. Some trade routes and thus, ports of origin, pose higher risks for trafficking of illicit goods and, therefore, require a degree of insider help to have shipments of illicit goods pass through the seaport supply chain (EMCDDA et al., 2019, p. 13; EMCDDA et al., 2022).

The human factor

One of the most vulnerable characteristics of the seaport and the supply chain is the human factor, which has been noted in all case studies and high-level interviews ([35]). More generally, this vulnerability is driven by the knowledge

([32]) Interviews with private and public stakeholders, February and March 2024 (Roks et al., 2020, p. 174).
([33]) Port of Piraeus, Port of Algeciras, Port of Antwerp-Bruges, Port of Rotterdam.
([34]) The high volumes of throughput were also mentioned by one respondent of the survey as a reason why it is difficult to tackle corruption risks.
([35]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Cartagena, Port of Venice; interviews with private and public stakeholders, February and March 2024.

of organised crime groups (OCGs) related to the actors that play a crucial role in processing containers, conducting checks and controlling entry to and exit from the seaport (Roks et al., 2021, pp. 56–57; Sergi, 2020, p. 197; Jancsics, 2019, pp. 3–4; Roks et al., 2020, pp. 182–183; Eski et al., 2017, pp. 3–4). Zooming into the specific corruption vulnerabilities of the human factor, three aspects stand out.

First, non-automated container processing requires more human involvement, which has been observed to increase corruption vulnerabilities and opportunities for OCGs ([36]). For example, during the offloading and placement of containers, stevedores and crane operators can be approached by OCGs to assist in placing containers in favourable and accessible locations in the terminal for picking up illicit goods later on ([37]).

Second, access to critical information such as containers selected for checks or the location of containers (with illicit goods) is not permanently restricted to a limited number of employees. In some cases, different teams working in the terminal have access to this information due to working in shifts ([38]). Broad access to critical information reduces oversight and might present more corruption opportunities for OCGs, as it is more difficult to link an employee to the leaked piece of information (Sergi, 2020, pp. 16–18, pp. 197–198; Europol, 2023, pp. 17–18). Third, transporters (e.g. truck drivers, train conductors, inland shipping captains), responsible for picking up the containers from the terminal for further transport, are particularly vulnerable and are therefore usually approached and bribed by OCGs. This has been identified specifically in relation to PIN codes ([39]) used to retrieve containers with illicit goods, or to bring in extractors to the port.

Social communities around the port

The role of the social communities in and around seaports is also relevant. The communities of people working in and for the seaport generally have long-standing relationships with the port and are generally proud and protective of the related seaport ([40]).

However, close-knitted seaport communities also pose substantial challenges and vulnerabilities related to corruption. It is not uncommon in certain seaports for staff to be hired through (in)direct family ties or recommendations. The connections of the close community also pose a vulnerability to corruption in light of procurement. Here, similar dynamics as those described above are at play whereby contracts are allocated to stakeholders that are part of the seaport community, rather than through transparent procurement procedures.

In addition to these vulnerabilities, there are socioeconomic factors that render the social communities around the port vulnerable to corruption. Examples of these factors are manifold but include, for example, high unemployment rates around the port ([41]), debt-related issues ([42]), poverty (Centrum Kinderhandel en Mensenhandel et al., 2021, p. 30) and a general sentiment of low trust in the government and its actions ([43]). These elements make some members of port communities susceptible to different forms of corruption.

([36]) Port of Algeciras, Port of Piraeus.
([37]) Port of Algeciras, Port of Piraeus.
([38]) Port of Algeciras; interviews with public stakeholders, February and March 2024.
([39]) Unique PIN codes are used by shippers and freight forwarders to securely release the container for onward transport by truck drivers at the port of arrival.
([40]) As seen in all case studies.
([41]) Port of Algeciras, Port of Piraeus, Port of Venice.
([42]) Port of Rotterdam, Port of Antwerp-Bruges (Eski et al., 2017, pp. 5–6, p. 17).
([43]) Port of Rotterdam, Port of Antwerp-Bruges.

Role of politics in the seaport

Whereas the focus of the study at hand is to identify corruption vulnerabilities in the operations of the seaport supply chain, it has become apparent that in some seaports the role of politics also creates vulnerabilities. These corruption vulnerabilities seem to predominantly impact the risk of procurement-related corruption and the ambitions of the seaport being driven by political interest ([44]).

Factors hindering an effective approach to the fight against corruption in seaports

In addition to the features in the seaport that pose direct vulnerabilities related to corruption, factors that hinder an effective approach against corruption have been identified. These factors indirectly contribute to the existence and persistence of corruption vulnerabilities in the supply chain. They concern the economic climate, the type, strategic location and size of the seaport, the cooperation between public and private actors in the seaport and legislation.

Economic climate

Seaports are hubs for (international) trade and transportation, serving as vital links in the logistical chain. In the pursuit of sustaining profitability, attracting business and maintaining a competitive position in the global trade, security considerations are occasionally overlooked, with efficiency taking precedence over security measures ([45]).

Some seaports struggle to keep pace with evolving modernisation while simultaneously upholding and enhancing all necessary security measures ([46]). The combination of these factors may lead to seaports prioritising economic interests over security considerations.

Size and location of the seaport

The size and location of a seaport indirectly impact the vulnerability to corruption in various ways. Firstly, the size of the seaport was mentioned as a key challenge in some of the larger seaports studied, such as in Rotterdam and Antwerp-Bruges ([47]), as it is virtually impossible to maintain complete oversight over the entire port premises and over personnel, companies and systems ([48]), thus creating vulnerabilities related to the trafficking of illicit goods both into and outside of the seaport ([49]).

While major seaports grapple with issues such as expansive terrain, smaller seaports face different challenges that impact their vulnerability to corruption. They face resource constraints that impact their ability to actually conduct controls of the physical terrain and patrols ([50]). Additionally, smaller seaports are more likely prone to the waterbed effect resulting from larger seaports around them stepping up security measures ([51]).

([44]) Port of Cartagena, Port of Algeciras; interviews with private stakeholders, March 2024 (GI-TOC et al., 2021, pp. 56–57; Sergi, 2020, pp. 22–23).
([45]) Interviews with private and public stakeholders, February and March 2024 (GI-TOC et al., 2021, pp. 40–45; Roks et al., 2020, pp. 182–184).
([46]) Port of Piraeus.
([47]) Rotterdam encompasses 467.4 million twenty-foot equivalent units and 12.5 hectares, and Antwerp-Bruges encompasses 13.5 million twenty-foot equivalent units and 14.65 hectares.
([48]) Interviews with public and law enforcement stakeholders, February and March 2024 (Roks et al., 2020, pp. 184–185). This was also mentioned by survey respondents.
([49]) Port of Piraeus.
([50]) Port of Piraeus, Port of Antwerp-Bruges.
([51]) Port of Cartagena (GI-TOC et al., 2021, pp. 39–40).

Secondly, the volumes of throughput affect the vulnerability to corruption in seaports ([52]). Seaports that see a higher throughput generally face more complex and elaborate processes and security measures, thus increasing the need for insider help ([53]). On the other hand, seaports with less throughput generally face fewer resources dedicated to security measures in the seaport and, as a result, tend to experience more weaknesses in their seaport landscape, providing opportunities for corruption ([54]).

Type of port

The main vulnerability linked to the ownership of the seaport is the varying degrees of obligations and policies for security, integrity and transparency. In privatised seaports, economic interests might prevail as the private entities owning the seaport are, naturally, inclined to favour efficiency over security.

Moreover, in privatised seaports, the public bodies tasked with fighting crime and corruption are dependent on the private stakeholders owning the seaport to implement their tasks ([55]) (Sergi, 2020, p. 18). The law enforcement authorities therefore rely on and are guided by the port management companies. This may delay the inspection and decrease the transparency of port operations ([56]). While landlord seaports might have more (harmonised) security policies, they remain vulnerable to crime and corruption, as the actual implementation and monitoring generally falls within the responsibility of private companies ([57]). This makes it challenging to ensure consistency in anti-corruption and security measures and may lead to an overlapping of accountability for security-related activities.

Public–private cooperation

Challenges in cooperation between public and public–private actors have been observed across the case studies and high-level interviews, as each port stakeholder has a demarcated responsibility in a specific part of the chain and therefore they rely heavily on each other ([58]) (Sergi, 2020, pp. 16–18, pp. 22–23). This configuration leads to a complicated basis for effective cooperation.

The principal corruption vulnerabilities concern the lack of oversight and transparency due to limited information sharing, trust issues and conflicting interests between public actors. These loopholes and inconsistencies in public–private and public–public cooperation impact the ability of public and private actors to effectively address crime (and corruption in particular). More controls and checks have significant economic effects on companies, which often bear the costs for these checks ([59]) (Sergi, 2020, pp. 16–18, pp. 26–27), thus underscoring the delicate balance between economy and security in seaports.

([52]) The high volume of throughput is also mentioned by one survey respondent as reason why corruption is difficult to tackle.
([53]) Port of Rotterdam, Port of Antwerp-Bruges (Antonelli, 2021, p. 164).
([54]) Port of Venice.
([55]) Port of Piraeus.
([56]) Port of Piraeus.
([57]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Venice.
([58]) Interviews with public and law enforcement stakeholders, February and March 2024.
([59]) Port of Algeciras, Port of Venice.

Legislation

Regarding corruption vulnerabilities posed by suitable legislation (or the lack thereof), two elements stand out. First, the International Ship and Port Facility Security Code (ISPS Code) (Regulation (EC) No 725/2004) is repeatedly mentioned as a weak link in seaports' anti-corruption (and anti-organised crime) approach ([60]). Given that the fundamentals of the ISPS Code lie in a counterterrorism response, the risks of OCGs' infiltration are not sufficiently covered by the code. The second vulnerability identified in terms of legislation is the restrictions with regards to information sharing. Due to these restrictions, cooperation is sometimes negatively affected ([61]).

Corruption vulnerabilities in the port supply chain

The following section of this article focuses on the corruption vulnerabilities in specific steps in the seaport supply chain, as presented in Figure 13.1 above.

It is essential to reiterate here that the supply chain has been designed based on trade from non-EU countries into EU seaports and with a prime focus on container trade. Furthermore, before corruption vulnerabilities are explained for each step of the supply chain, it is important to underline that the legitimate activities taking place at each step have also been presented to provide a clear overview of the supply chain.

Step 1: Goods packed into a container at the production location

Legitimate activities

The supply chain starts when the goods to be transported are packed into a container at the production location. In this instance, the goods are physically put into the container that will be shipped. Staff employed by the exporting company are involved in this step, physically packing goods into the container.

Corruption vulnerabilities

The key corruption risks in this step concern the lack of standardised rules and protocols for packaging at the production location. OCGs therefore use the prevailing modus operandi (MO) of hiding illicit goods among high-volume shipments. Corruption is used to gain the assistance of production and warehouse personnel to add the illicit goods to the containers ([62]).

Step 2: Container transported from production location to port of departure

Legitimate activities

After loading the goods into the container, the container is transported to the seaport of departure. The container is brought to the terminal, where it will be picked up by the vessel that will transport it to the intended destination. The person or company transporting the container plays a key role in this step.

([60]) Predominantly mentioned in Port of Rotterdam and Port of Antwerp-Bruges.
([61]) Port of Piraeus, Port of Antwerp-Bruges; interviews with private and public actors, February and March 2024.
([62]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with private stakeholders, March 2024 (GI-TOC et al., 2021, pp. 44–45; OCCRP, 2019); 15 respondents in the survey (n = 16) also recognised this risk. According to the survey findings, transport companies and warehouse personnel emerged as the most susceptible to corruption.

Corruption vulnerabilities

The key vulnerability in this step is the physical transport of the container from the production location to the terminal. During this transport, OCGs might bribe the driver to make additional stops to load illicit goods into the container ([63]) (GI-TOC et al., 2021, pp. 43–45; OCCRP, 2019; Stockholm International Peace Research Institute et al., 2012, pp. 35–36). It is worth noting that OCGs could also approach the container without the active involvement of the driver, when the vehicle is stationary in a car park. ([64])

Step 3: Container loaded from the terminal onto the vessel

Legitimate activities

Once the container has been transported from the production location to the terminal, it is loaded into a vessel for transport. The customs authority oversees handling the export declaration of the goods and releasing the container for departure. The terminal personnel ensure the container transfer from the terminal onto the vessel.

Corruption vulnerabilities

In this step, the terminal personnel could be bribed by OCGs to add illicit goods into the container whilst it is stored in the terminal (i.e. the so-called rip-on/rip-off method). Alternatively, they could be bribed to look the other way and let criminals add illicit goods into the containers before loading them onto the vessel ([65]). In addition, the limited screening of exported goods (container loads and ro-ro loads) provides a bigger 'window of opportunity' for illicit goods to be loaded onto the vessel.

Step 4: Vessel sails to destination

Legitimate activities

This step focuses on what occurs on sea. After the container has been loaded onto the vessel, it starts its journey to the port of destination. The main actor in this step is the vessel's crew.

Corruption vulnerabilities

The corruption vulnerabilities identified in this step concern the vessel itself and its route. First, ship personnel are vulnerable to corruption, for example, allowing the hiding of illicit goods in cabins ([66]) (GI-TOC et al., 2021, pp. 44–45). Similarly, ship personnel can allow OCGs to weld underwater constructions to a ship's hull (e.g. dispatchable torpedoes), where illicit goods can be hidden. This allows the OCGs to evade security checks at the seaport and decreases the need to bribe dock workers to extract illicit goods (GI-TOC et al., 2021, pp. 44–45).

Second, it is evident that there is a risk of OCGs influencing ship personnel to make additional stops whilst at sea or diverting the vessel from its original route ([67]). In addition, corrupt ship personnel use the drop-off method whilst at sea. In this case, a corrupt ship employee drops illicit goods into the sea, for example, a package of cocaine (as

([63]) Fifteen respondents of the survey recognised this risk ($n = 16$).
([64]) Port of Piraeus.
([65]) Port of Algeciras (GI-TOC et al., 2021, pp. 43–45); 14 respondents of the survey recognised this risk ($n = 16$).
([66]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Algeciras, Port of Venice, interviews with law enforcement agencies, February 2024.
([67]) Port of Antwerp-Bruges.

cocaine floats), which are then picked up by OCGs in smaller speedboats ([68]) (Politico, 2021). This is particularly appealing for OCGs as the vessel is rather isolated at sea, and there are no authorities on site (Europol, 2023, pp. 13–14; GI-TOC et al., 2021, pp. 42–44).

Step 5: Relevant actors in the port of arrival are notified about the expected arrival of the vessel

Legitimate activities

The port authority, customs and other relevant authorities at the seaport of arrival receive information about the container from the port of origin. Customs authorities then start to prepare the clearance procedure for the container.

Corruption vulnerabilities

The corruption vulnerabilities in this step predominantly lie with customs authorities, shippers, ship agents and freight forwarders, who are the key actors involved in the documentation of shipments, making these groups vulnerable to corruption ([69]) (Roks et al., 2020, p. 182; Jancsics, 2019, pp. 3–4; Langlois et al., 2022, pp. 296–298; GI-TOC et al., 2021, pp. 42–43; Europol, 2023, p. 10; EMCDDA et al., 2019, p. 7) as they are responsible for sending the entry summary declaration (ENS) to the customs authorities at the seaport of arrival. There is a risk of OCGs bribing these private actors to falsify the ENS to import illicit goods.

Step 6: Vessel arrives at quay

Legitimate activities

In this step, the vessel arrives at the quay of the terminal. The container is now on the vessel at the quay of the seaport of arrival, waiting to be placed in the terminal.

Corruption vulnerabilities

Vulnerability to corruption involves the personnel overseeing or managing the vessels waiting at the quay, as OCGs could bribe them to turn a blind eye to other bribed personnel extracting illicit goods from the vessel ([70]) (Roks et al., 2020, p. 182; Jancsics, 2019, pp. 3–4).

Moreover, the drop-off of packages of drugs by corrupt ship personnel ([71]) into the water or in smaller speedboats, picked up by divers recruited by OCGs, is a prevalent MO also at this step ([72]) (GI-TOC et al., 2021, pp. 44–45).

([68]) Port of Piraeus, Port of Algeciras, Port of Venice; 14 respondents of the survey recognised this risk ($n = 16$).
([69]) Port of Piraeus, Port of Antwerp-Bruges, Port of Rotterdam, Port of Algeciras, Port of Venice. Findings from the survey: customs authorities in particular were perceived as vulnerable to corruption by the survey respondents (9 out of 14).
([70]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Venice; 13 respondents of the survey recognised this risk ($n = 15$).
([71]) Often the same ship personnel that has already been corrupted at the port of origin.
([72]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Venice; interviews with law enforcement agencies, February 2024.

Step 7: Terminal operator unloads the vessel and parks the container at the terminal

Legitimate activities

Once the vessel is moored at the terminal, the terminal operators unload the containers and place them in the terminal. The goods are then assigned to a specific customs procedure, depending on where the containers are coming from (intra-EU or non-EU country) (European Commission: Directorate-General for Trade and Economic Security, 2026).

Corruption vulnerabilities

The corruption vulnerabilities linked to the human factor seem rather critical at this step, as observed across the case studies and high-level interviews ([73]). Subcontracting and independent and occasional workers render terminal personnel an increasingly vulnerable group due to difficulties in screening them. Additionally, the monetary compensation offered by OCGs is very high (ranging from EUR 25 000–200 000) ([74]). This increases the attractiveness of engaging in corruption for terminal personnel.

Influencing terminal personnel in order to extract illicit goods from the containers is therefore attractive for OCGs. OCGs use forms of corruption with few widely known MOs, such as the rip-on/rip-off method, Trojan Horse containers and hotel containers ([75]). Notably, limited port surveillance grants potential access to OCGs to illicit goods prior to customs inspections.

Step 8: Customs checks paperwork and decide based on the risk management system which containers to select for checks

Legitimate activities

In this step, the container is parked in the terminal and is waiting for customs clearance. The customs authority check the necessary documents and decide whether to release the container to the transport company.

In addition, the customs authority uses a risk management system to determine which containers to check. If the container is selected for a check, it can be either moved to a customs inspection area or checked on the spot by authorities.

Corruption vulnerabilities

Corruption vulnerabilities in this step are mainly linked to customs authorities and other actors conducting checks in the seaport. Authorities might be bribed to 'turn a blind eye' if they spot suspicious activity or illicit goods. Additionally, customs officers sometimes have discretion over which containers to physically check due to shortages

([73]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus, Port of Algeciras, Port of Venice; interviews with private and public stakeholders, February and March 2024.
([74]) Port of Rotterdam, Port of Antwerp-Bruges, Port of Piraeus.
([75]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with public and law enforcement stakeholders, February and March 2024.

in personnel and time restrictions. This coupled with the lack of adherence to the four-eye principle and rotation of customs officers, contributes to the corruption vulnerabilities ([76]).

Second, customs authorities can also be bribed to select containers other than the containers containing illicit goods for checks or to speed up the processing of the container to avoid physical checks ([77]) (OCCRP, 2019). In some cases, the notification period of selecting a container for checks is relatively long, which allows corrupt employees to notify OCGs to extract the illicit goods before the checks are conducted (through the rip-on/rip-off method or the switch method) ([78]) (Jancsics, 2019, pp. 3–4).

Step 9: Container is loaded onto onwards transport towards importer/destination

Legitimate activities

The container is released to the transport company. The freight forwarder usually organises the transport of the container.

Corruption vulnerabilities

Regarding the transport of the container, the main vulnerabilities identified lie in road transport, non-automated access to the terminal and the lack of monitoring of railway systems. Authorities are not allowed to check the driver's cabin, which makes it harder to catch OCGs transporting illicit goods.

In addition, the use of PIN codes is often subject to fraud. This allows the OCGs to retrieve the container with illicit goods from the terminal either themselves or with the help of a bribed transporter ([79]) (Europol, 2023).

Step 10: Arrival at the importer/destination

Legitimate activities

After the transport company has picked up the container, it is transported to the importer. The importer then usually organises the unloading of the container at the final destination.

Corruption vulnerabilities

The main corruption vulnerability in this step concerns the importer and the warehouse personnel who may have been bribed or recruited by OCGs to add or remove illicit goods from the container.

([76]) Port of Antwerp-Bruges, Port of Rotterdam, Port of Venice. Respondents of the survey recognised this risk ($n = 15$).
([77]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with private stakeholders, February and March 2024.
([78]) Port of Antwerp-Bruges, Port of Rotterdam, Port of Venice; interviews with public stakeholders, February and March 2024.
([79]) Port of Rotterdam, Port of Antwerp-Bruges; interviews with public and private sectors, February and March 2024.

Conclusion

Combining the findings across the different seaports studied, the insights gathered from beyond those case study seaports and the overarching desk research and interviews provides an overview of a variety of corruption vulnerabilities.

The identified vulnerabilities in seaports are directly linked to the supply chain, but also to more structural, indirect elements in and around the seaport that increase the vulnerability to corruption or, in turn, hinder an effective approach to corruption. Furthermore, this article has shown that there is a wide range of different seaports in the EU, with different features, facing different types of challenges.

One of the key conclusions from the article is that the vulnerabilities related to corruption in the seaport supply chain are manifold, but are only one piece of the puzzle. The vulnerabilities in the supply chain predominantly pertain to the involvement of personnel, loopholes in (legal) processes and systems, and lack of oversight.

Compared with corruption-related vulnerabilities in the supply chain, the underlying and more structural elements and features in and around seaports that create vulnerabilities for corruption are generally more difficult to address, but risk being more impactful. These vulnerabilities are the consequence of more transversal issues such as the degree of human involvement in the seaport, the degree of digitalisation, the type and origin of the cargo and throughput, the role and composition of social communities around the seaport and the role of politics in the seaport. These elements are not directly linked *per se* to specific steps of the seaport supply chain but instead affect multiple steps across the supply chain.

These difficulties are further intensified by a series of factors hindering an effective and efficient approach to corruption in seaports. Such factors include, among others, the size and location of the seaports, the prioritisation of efficiency over security, the ownership of seaports, cooperation between public authorities in the seaport, the degree of collaboration between public and private bodies, and legislation. While these factors do not directly translate into vulnerabilities to corruption in the seaport supply chain, they do affect the ability of addressing corruption in the seaport effectively.

These findings provide useful food for thought for the law enforcement community as it strives to respond effectively to the ever-growing phenomenon of corruption and infiltration of organised crime within European ports.

Overall, it has become evident that an all-encompassing set of corruption vulnerabilities applicable to all seaports across the EU is non-existent. Specific vulnerabilities, and their intensity and operational details, differ substantially between seaports. Taking this into account, four key findings must guide the efforts in addressing the vulnerabilities to corruption in EU seaports when moving ahead.

First, tailored approaches to address the vulnerabilities in the various seaports are required, as a generic strategy would overlook the specificities of the needs in seaports, such as the level of digitalisation, human involvement, the political priorities and available resources. Strategies to address corruption vulnerabilities in seaports must take these specificities into account and design tailor-made measures. Second, the vulnerabilities related to corruption

in seaports must not be addressed from the perspective of a single seaport or only at the national level. Instead, seaports should be understood as a broader group of logistical hubs across the EU. Indeed, an EU-wide approach and EU-level investments in port security would have to be adopted to ensure an equal level playing field, and thus an equal minimum level of resilience across the EU and single market. This rationale could be extended beyond EU seaports in the future to also include non-EU seaports.

Third, an effective approach to combating corruption in seaports would not only include repressive measures focused on specific operational vulnerabilities in the seaport supply chain, but would also address the more structural challenges present in and around seaports. In this sense, it could be beneficial to dedicate resources to prevention strategies.

Fourth, an update of the ISPS Code would allow more effective oversight of the implementation of appropriate security measures in the seaport ([80]). Such an update would be most effective to avoid a waterbed effect whereby OCGs shift activities to ports with less strict legislation.

These key findings and suggestions for a way forward shall be considered in the identification and selection of practices that aim to tackle corruption in EU seaports, and in the definition of recommendations for the establishment of an EU port supply chain integrity standard.

References

Antonelli, M. (2021), 'An exploration of organized crime in Italian ports from an institutional perspective – Presence and activities', *Trends in Organized Crime*, Vol. 24, pp. 152–170, https://doi.org/10.1007/s12117-020-09400-z.

Centrum Kinderhandel en Mensenhandel, Leito, T. L. M., van Bemmel, S. R. and Noteboom, F. (2021), *Het misdrijf voorbij – Een verkenning naar criminele uitbuiting in Rotterdam*, Capelle aan den IJssel, https://www.hetckm.nl/wp-content/uploads/2023/03/CKM-Rapport-2021-Het-misdrijf-voorbij.pdf.

EMCDDA and Saggers, T. (2019), 'An assessment of the extent of Albanian(-speaking) organised crime groups involved in drug supply in the European Union: characteristics, role and the level of influence', https://www.euda.europa.eu/system/files/attachments/12102/EDMR2019_BackgroundReport_Albania nSpeakingOCGs.pdf.

EMCDDA and Europol (European Union Agency for Law Enforcement Cooperation) (2022), EU Drug Market: Cocaine, https://www.euda.europa.eu/publications/eu-drug-markets/cocaine_en.

Eski, Y. and Buijt, R. (2017), 'Dockers in drugs: Policing the illegal drug trade and port employee corruption in the Port of Rotterdam', Policing: A Journal of Policy and Practice, Vol. 11, Issue 4, pp. 371–386, https://doi.org/10.1093/police/paw044.

([80]) It should be noted that Belgium EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) introduced a new maritime security law on 1 January 2023 (*Wet tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging*, Belgian Official Gazette, 26 October 2022), which lays down stricter measures than the ISPS Code.

European Commission: Directorate-General for Trade and Economic Security (2025), 'Customs clearance documents and procedures', Access2Markets website, https://trade.ec.europa.eu/access-to-markets/en/content/customs-clearance-documents-and-procedures.

European Parliament and Council of the European Union, Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6, ELI: http://data.europa.eu/eli/reg/2004/725/oj.

European Parliament: Directorate-General for Parliamentary Research Services, Bąkowski, P. and Voronova, S. (2017), *Corruption in the European Union – Prevalence of corruption, and anti-corruption efforts in selected EU Member States – In-depth analysis*, European Parliament, https://data.europa.eu/doi/10.2861/071091.

Europol (2023), 'Criminal networks in EU ports – Risks and challenges for law enforcement', https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint.

Europol (2021), European Union Serious and Organised Crime Threat Assessment – A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

GI-TOC (Global Initiative Against Organized Crime), InSight Crime, McDermott, J., Bargent, J., and den Held, D. (2021),, *The Cocaine Pipeline to Europe*, GI-TOC, Geneva, https://globalinitiative.net/wp-content/uploads/2021/02/The-cocaine-pipeline-to-Europe-GI-TOCInsightCrime.pdf.

Jancsics, D. (2019), 'Border Corruption', *Public Integrity*, Vol. 21, Issue 4, pp. 406–419, https://doi.org/10.1080/10999922.2019.1581043.

Langlois, F., Rhumorbarbe, D., Werner, D., Florquin, N., Caneppele, S. et al. (2022), 'International weapons trafficking from the United States of America: A crime script analysis of the means of transportation', *Global Crime*, Vol. 23, Issue 3, pp. 284–305, https://doi.org/10.1080/17440572.2022.2067847.

OCCRP (Organized Crime and Corruption Reporting Project) (2019), 'Albanian drug suspect's banana bonanza', OCCRP website, 16 December 2019, https://www.occrp.org/en/investigation/albanian-drug-suspects-banana-bonanza.

Poseidon, Saarijärvi, J., Helemons, S., op t' Hoog, G., Steensma, J. et al. (2024), 'Study on corruption vulnerabilities in the EU seaports supply chain', https://poseidon.safe-europe.eu/wp-content/uploads/2024/10/POSEIDON_Study-on-corruption- vulnerabilities-in-the-EU-seaports-supply-chain.pdf.

Poseidon (2023), 'POSEIDON – POrtS unitED Against corruption', Poseidon website, https://poseidon.safe-europe.eu/.

Roks, R., Bisschop, L. and Staring, R. (2021), 'Getting a foot in the door – Spaces of cocaine trafficking in the Port of Rotterdam', *Trends In Organized Crime*, Vol. 24, pp. 171–188, https://doi.org/10.1007/s12117-020-09394-8.

Sergi, A. (2020), *The Port-Crime Interface: A report on organised crime and corruption in seaports*, University of Essex, London, https://repository.essex.ac.uk/30303/1/EBOOK_PORT_CRIME.pdf.

Stockholm International Peace Research Institute, Griffiths, H. and Jenks, M. (2012), *Maritime Transport and Destabilizing Commodity Flows*, Stockholm, https://www.sipri.org/sites/default/files/files/PP/SIPRIPP32.pdf.