Container Security: Combating the Rip-On Rip-Off technique and the Blockchain Technology

By Elena-Sofia Cesario

Publication Details

Published: February 18, 2021

Publisher: Invictus Corporation Ltd.

Department: Security Challenges at Seaports

Author: Elena-Sofia Cesario

Editors: Harshita Bhattacharya, Avani Bohara, Ajatshatru Bhattacharya

Produced, published and distributed by INVICTUS CORPORATION LTD., The Hague, The Netherlands

Website: https://invictuscorp.org/

The registered company address is: New World Campus, Spaarneplein 2, 2515 VK The Hague, The Netherlands

Table of Contents

Keywords: Container, Seal, Security, Rip-Off, Rip-On, Corruption, Blockchain, Maritime, Shipping, Seaports

List of Abbreviations

Abbreviation	Description
1PL	First Party
2PL	Second Party
3PL	Third-Party
4PL	Fourth Party
AEO	Authorised Economic Operator
C-TPAT	Customs-Trade Partnership Against Terrorism
CCP	Container Control Program
CTU	Cargo Transport Unit
CTU Code	Cargo Transport Unit Code
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EU	European Union
GISIS	Global Integrated Shipping Information System
GPS	Global Positioning System
H Seal	High-Security Seal
ICSO	International Container Standard Organization
ILO	International Labour Organization
IMO	International Maritime Organization
IoT	Internet of Things
ISM	International Safety Management
ISO	International Organization for Standardisation
ISPS	International Ship and Port Facility Security
OCGs	Organised Crime Groups
SAFE Framework	Standards to Secure and Facilitate Global Trade Framework
SOLAS	Safety of Life at Sea
TEU	Twenty Equivalent Unit
UNCTAD	United Nations Conference on Trade and Development
UNECE	United Nations Economic Commission for Europe
UNODC	United Nations Office on Drugs and Crime
VGM	Verified Gross Mass
WCO	World Customs Organization
WCO	World Customs Organization

1. Introduction

Due to the complex nature of international supply chains, it is no surprise that at any given time, there are numerous parties involved in the trade process. Each party has a unique role and a different set of responsibilities and liabilities, making for an intricate operational framework. This complexity and intricacy allow nefarious Organised Crime Groups (OCGs) to infiltrate the supply chain, elude security and 'piggyback' off legitimate trade routes.

Container screening involves just 0.0005% of the overall containers arriving in seaports. Given the significant volumes, it is often challenging for authorities to notice if a container has been tampered with during its journey. Considering this low screening rate, one of the most commonly utilised modus operandi by the OCGs to benefit from legitimate trade and smuggle contraband is the 'Rip-On/Rip-Off' technique. In conjunction with corruption at seaports, this technique enables OGCs to use seaports such as the Port of Rotterdam to smuggle contraband into Europe.

In the recent decade, we have observed a sharp increase in the volume of international maritime trade. Many experts argue that traditional paper-based systems are inefficient and vulnerable to exploitation by the OCGs. For instance, the documents and container seals are susceptible to forgery, and it is often hard to allocate individual liability given the numerous parties involved. Various stakeholders involved in the process have identified container traceability, container seal security, and an increasing rate of corruption amongst port workers as the most prominent challenges in the current framework.

This report aims to provide a comprehensive overview of the 'Rip-On/Rip-Off' technique and how stakeholders could address the associated challenges. The report also highlights emerging technologies such as blockchain and its use within the traditional international maritime trade framework. Finally, the report addresses the importance of container seals in the trade process while highlighting the need for a more automatised operational framework.

2. Methodology

Data surrounding the Rip-On/Rip-Off technique must be considered through the lenses that 0.0005% of containers are screened worldwide in seaports. Given the nature and importance of container security and seaport security, Organized Crime Groups exploit this lack of infrastructure and capacity for their nefarious schemes.

In order to address the subject matter efficiently and effectively, the report relies on a mixed research methodology. More specifically, this report utilises doctrinal and empirical research methodologies. Doctrinal research allows for an evaluation of the international framework relating to container security and its interaction with blockchain technology. An empirical research methodology is subsequently utilised to gain practical insights and verify the findings.

Chapter 3 provides a doctrinal analysis of the current challenges that seaport security faces regarding OCG's illegal business in seaports, including its primary *modus operandi*, the Rip-On/Rip-Off technology. Furthermore, it considers several salient points on the Rip-on/Rip-Off at seaports and its role in undermining container security to provide a comprehensive summary of the *modus operandi* process.

Building on this, Chapter 3.2. provides a description of container seals and their usage within the transnational framework. The section further outlines the goals, practical frameworks, methods for a tamper-proof system by the International Organization for Standardization, and the different types of container seals in the market and their identification code. Following this, the report illustrates various challenges associated with container tracking and how stakeholders are looking to provide a suitable tracking device within the container.

Chapter 4 takes a turn towards empirical legal research, considering corruption cases at the Port of Rotterdam in a time frame from 2010 until 2019. It will primarily employ a qualitative empirical approach, conducting document analysis and case analysis to access the Rip-On/Rip-Off technique's role in bribing seaport workers for its success.

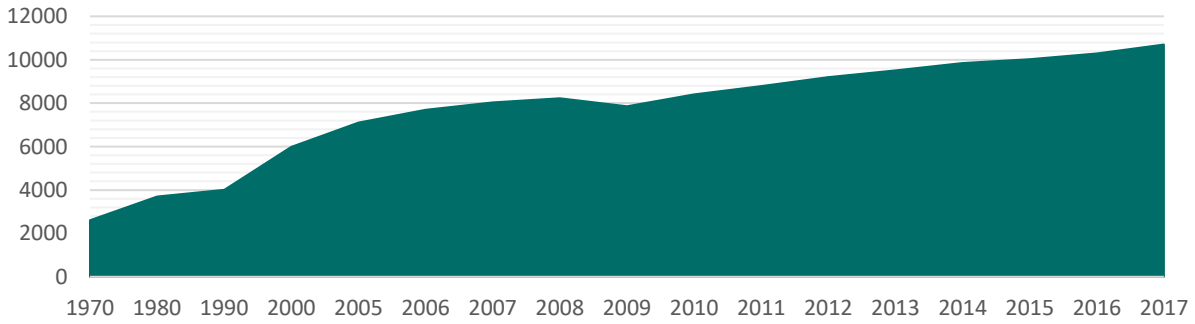
A combined approach of qualitative and doctrinal research is the most suitable to answer the relevant research question through a doctrinal analysis of container seals' role, empirical considerations of its effectiveness in making a tamper-proof container. The methodology effectively caters to defining the container seals' useful function and outlining the challenges posed by technological innovation. Moreover, the present research focuses on the goals, approaches, and new blockchain technology methods.

As technological developments pose novel legal challenges to the international community, it does help the maritime security field to tackle long-overdue illegal practices at seaports. Furthermore, within the automatisation of seaports, such unlawful practices could drastically diminish; however, since it is a new technology under development, research on such topics must be continuously revisited. This report ultimately aims to contribute to such literature.

3. The Rip-on/Rip-off technique

3.1. Container Security

World seaborne trade has seen a steady increase since 1980[1]; breaking in 2017 a threshold of 10.000 million tons.[2] More specifically, regarding global containerised trade, the UNCTAD estimates that 752.2 million of 20 foot-equivalent units (TEUs) were moved through ports worldwide in 2017. In 2018, seaports handled nearly 80% of the global trade of goods in terms of volume.[3] Authorities across the globe, such as but not limited to the International Maritime Organization (IMO) have long acknowledged the security challenges associated with this volume.

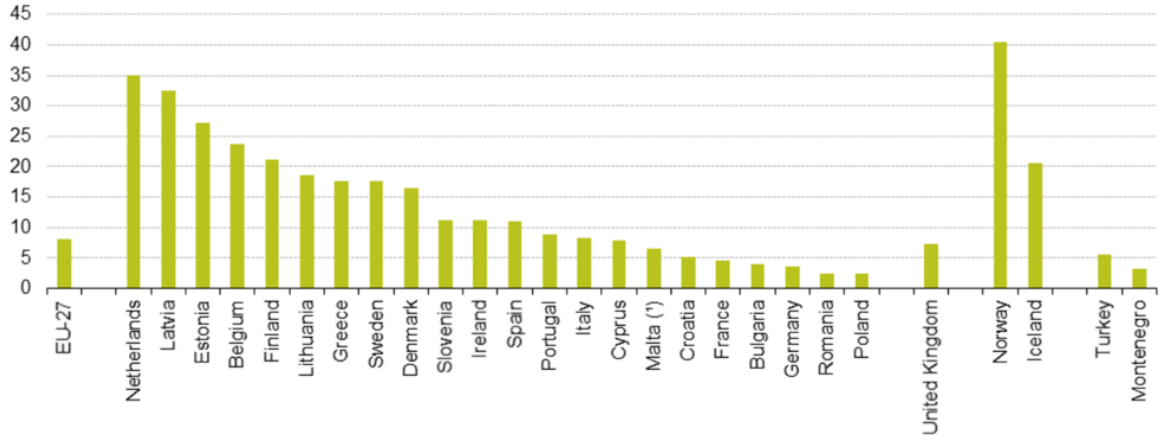


Graph 1: All Cargo (Crude oil, petroleum products and gas; main bulks; other dry cargo).[4]

In parallel with global container trade growth, criminal organisations are expanding their cross-border operations and finding innovative ways to circumvent security measures. From a microeconomic perspective, the motivation behind OCGs growth can be found in the increased (international) demand for illicit goods and the proliferation of 'retailers' and traders on the dark web. In addition to

[1] United Nations Conference on Trade and Development, 'Review on Maritime Transport 2018', 2018.
[2] Ibid.
[3] Ibid.
[4] United Nations Conference on Trade and Development, based on data supplied by reporting countries and as published on government and port industry websites, and by specialist sources. Notes: Dry cargo data for 2006 onwards were revised and updated to reflect improved reporting, including more recent figures and a better breakdown by cargo type. Since 2006, the breakdown of dry cargo into main bulks and dry cargo other than main bulks is based on various issues of the Shipping Review and Outlook, produced by Clarksons Research. Total estimates of seaborne trade figures for 2017 are based on preliminary data or on the last year for which data were available.

this growth in demand and ease of access, OCGs are also benefitting from globalisation and an increase in the global trade volume. Furthermore, considering the sheer volume of international maritime trade, it should come with no surprise that the OCGs would look to capitalise on existing legitimate transnational maritime trade routes for their nefarious schemes. For instance, the European Union (EU) handles around 11 million containers each year, of which barely 50.000 are adequately scanned which presents a unique low-risk cost-effective opportunity to OCGs.[5]



Graph 2: Gross weight (tonnes per inhabitant) of seaborne freight handled in all seaports (2018).[6]

To put things in perspective, these numbers indicate that mere 0.0005% of containers that arrive at European seaports are scanned. On the one hand, the large volume of legitimate goods makes it easier for OCGs to conceal contraband and minimise detection risk. On the other, this operational framework is highly cost-effective compared to other frameworks such as air transport for transnational smuggling. In a 2016 report, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) visualised air, land, and maritime drug trafficking routes between Latin America – Europe and Africa as utilised by various OCGs.[7]

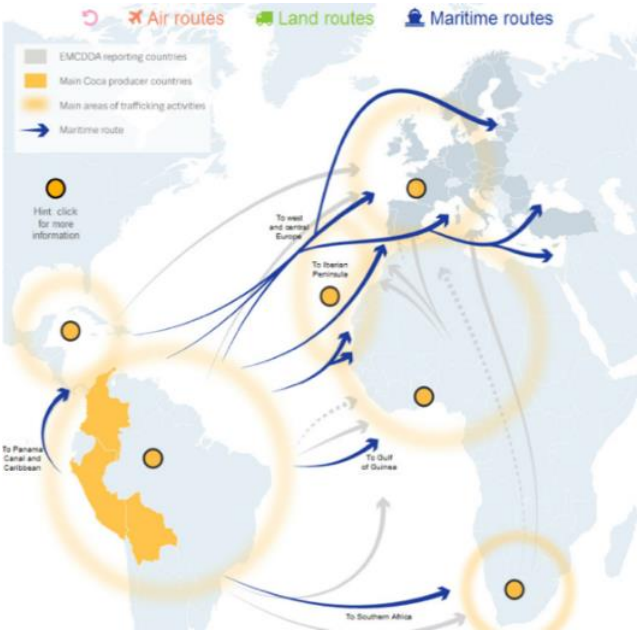


Image 1: Cocaine trafficking routes to EU

[5] Ibid; United Nations Conference on Trade and Development, 'Review on Maritime Transport 2018', 2018.
[6] EuroStat, 'Gross weight of seaborne freight handled in all ports', 2018, accessed September 1, 2020.
[7] European Monitoring Center for Drugs and Drug Addiction, 'Interactive map of cocaine trafficking routes to Europe' <https://www.emcdda.europa.eu/cocaine-trafficking-europe_en> accessed September 1, 2020.

Alongside various stakeholders, the international community has taken legislative and policy-driven measures to contain the growing transnational illicit trade and address emerging security vulnerabilities. For instance, *the International Convention for the Safety of Life at Sea (SOLAS)* was amended, and new chapters - namely *Chapter IX: International Safety Management (ISM) Code* and *Chapter XI-2: The International Ship and Port Facility Security (ISPS) Code* - were introduced to address some of the concerns mentioned above. Recognising that the seaports and stakeholders in the maritime supply chain process are migrating towards digitalisation, the IMO in 2017 published guidelines on Maritime Cyber Risk Management to safeguard shipping from current and emerging threats and vulnerabilities related to digitisation, integration and automation of processes and systems in shipping. More recently, in 2020, the IMO has further developed on these guidelines and published a comprehensive report on, '*Safe Transport of Containers*', where it not only acknowledges emerging practices of OCGs but has also developed a series of requirements to ensure safe shipping as well as guidance for packing and securing containers.[8]

3.1.1. OCGs Piggybacking

While efforts towards a more secure environment have been made, a uniform approach to container security at seaports globally might still be far away. Based on data aggregated by EMCDDA and Europol in their 2019 EU Drug Market Reports it is evident that the demand for illicit goods (more specifically narcotics) has seen a sharp uptrend and that the OCGs can meet the demand.[9] However, due to the complexity of the maritime supply chain and secretive nature of OCGs activities, it is hard to gauge the direct effect of these legislative efforts on the growth of the illicit markets or the associated security challenges.

As eluded above, OCGs prefer to infiltrate maritime trade routes due to the lower risk of detection and cost-effective concealment as well as transportation of contraband. OCGs look for existing maritime trade routes that lead them to their target seaport and aim to conceal their contraband alongside legitimate goods. This operational framework is often referred to as a 'piggyback ride'. Over the last decade, the OCGs have developed and refined various *modus operandi* and techniques within this operational framework. These include 'Rip-on/Rip-off', switching (containers), concealing contraband inside the container structure, drop-off, underwater attachments and semi-submersible attachments.[10] Some of these illegal actions are perpetrated by exploiting the means through which

[6] IMO, 'Safe Transport of Containers', accessed August 15, 2020. <http://www.imo.org/en/MediaCentre/HotTopics/container/Pages/default.aspx>.

[9] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol, 'EU Drug Markets Report 2019' (2019) Publications Office of the European Union.

[10] Ajatshatru Bhattacharya and Benjamin Peters, '*The Underwater War on Drugs: An overview of the Dutch Customs Diving Team*', 2020, Invictus Corporation Ltd.

containers are tracked and secured.[11] For instance, every container has a bill of lading, which states a very detailed list of its cargo; to avoid tampering during the shipment, containers are equipped with seals. It is essential to underline that these seals are no longer produced by government-run companies but by private companies.

Additionally, due to the complex multi-stakeholder operational framework, OCGs require assistance from seaport personnel to place and recover their illegal goods. To that end, the OCGs have also been exploiting the personnel increase needed to handle the increased trade at seaports by promoting corruption through extortion, coercion, bribery and other means.

3.1.2. The Rip-On/Rip-Off Technique

In the past years, 'Rip-On' has emerged as the most used technique to traffic illegal goods. The World Customs Organization (WCO) in 2008 defined this technique as selecting a container with a predefined route and legit cargo. With seaports workers' help, OCGs can place their illegal goods inside the container before the seal is applied at the port of departure. Then they will recover the content at the port of arrival and eventually use a fake seal to avoid clear signs of container tampering. A vital element of this *modus operandi* is the corruption of port employees at both ends.[12]

Procedurally, the OCGs identify a container destined for target location, say for instance Europe. Once it is selected, the OCGs carry out an assessment on its suitability – amongst other aspects, they look at the relevant procedures applicable to the container, the travel time, storage conditions. Once finalised, OCG Members or their associates (corrupt port workers) conceal the contraband in the container(s). Once it reaches Europe, there are two prerequisites for the success of their scheme. First, the OCG Members or their associates must have all the relevant container information such as but not limited to the location of the container, details for the container seal (in the event of 're-locking', more on this below), relevant schedules. Second, the individuals in question also require 'easy' access to the container terminal.

In the event, the collection must take place at a transit location, or while the container is still on its journey, OCGs or their associates share information on the original container seal used is provided to the Rip-Off team which then makes a duplicate seal with the same specifications such as the same serial numbers or identifiers. During the retrieval process, the original seal is broken, and contraband is retrieved after which the container is sealed with the duplicate seal to avoid any signs of tampering. An interesting peculiarity of this *modus operandi* is that, sometimes, when the container seal

[11] Ibid..
[12] EUROPOL, 'EU Drug Markets Report – a Strategic Analysis', 2019 page 62.

information is available in advance, the loading team places the duplicate seal within the illicit cargo, to enable the counterpart at the seaport of arrival to reseal as necessary.

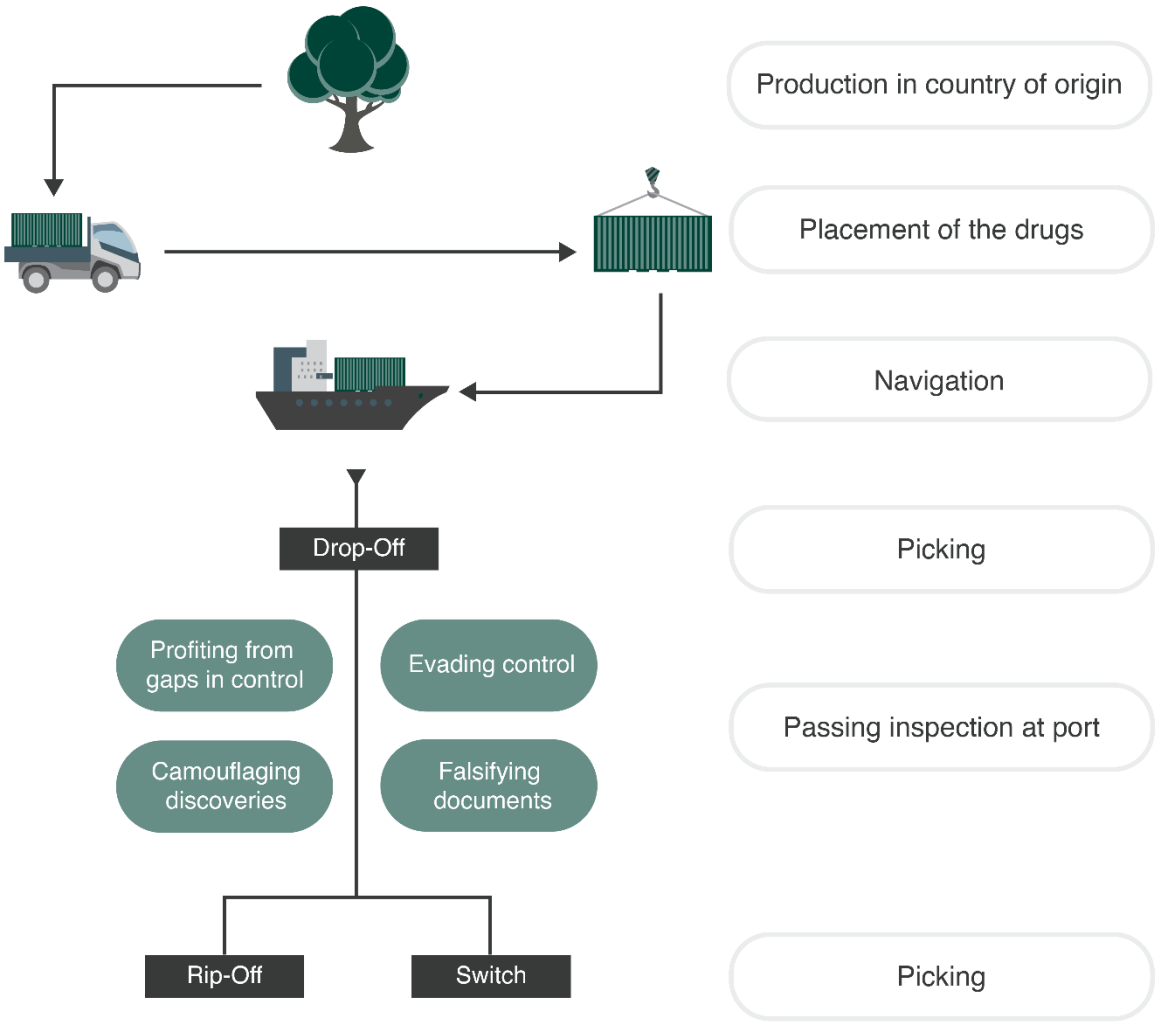


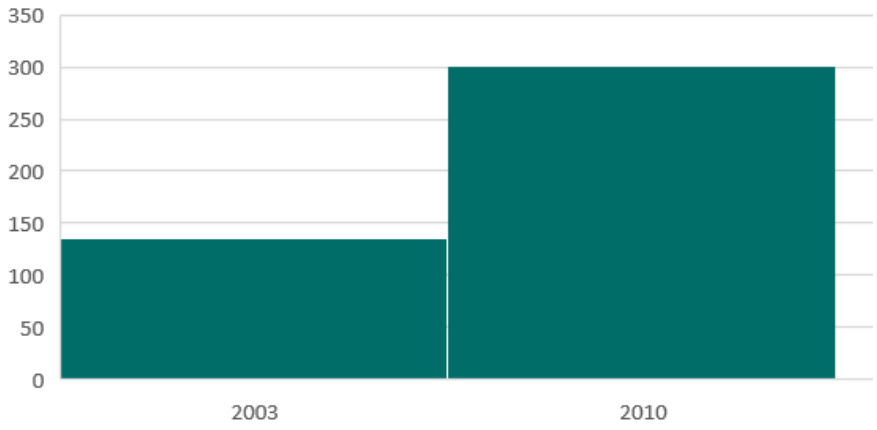
Image 2: An overview of the Rip-On/Rip-Off modus operandi.[13]

Since the contraband has to be collected physically from the container, it is quintessential for the container to be either in a secluded region or an area with less supervision i.e. a low risk zone. One could argue that the entire operation revolves around having access to strategic port areas at both the port of departure and arrival. Furthermore, since a piggyback framework requires legitimate cargo to be present alongside contraband, it is often the case that neither the consignee nor the shipper is aware of the tampering or the contraband placed within the container(s).[14] It is perhaps interesting to note that OCGs often target containers with perishables (for example fruits and vegetables) since they follow accelerated customs procedures and are often fast-tracked for other procedures. At the

[13] H.J.M. Staring, L.C.J. Bisschop, R.A. Roks, E.G. Brein and H.G. van de Bunt, 'Drug Crime in the Port of Rotterdam: about the phenomenon and its approach', 2019 page 23.
[14] United Nations Office On Drugs and Crime, 'CCP Glossary of Terms'. <https://www.unodc.org/ropan/en/BorderControl/container-control/ccp-glossary-of-terms.html>, accessed August 25 2020.

time of writing this report, findings suggest that this *modus operandi* is primarily used to smuggle cocaine and cannabis.[15] It is estimated that 3.6 million adults (between 15-64) in Europe used cocaine in 2019 alone.[16] Building up from the European Monitoring Centre for Drugs and Drug Addiction, after cannabis, it is the second most seized drug.[17]

Analysing the corruption requirement further, it becomes evident that OCGs have become extremely persuasive in order to corrupt workers and law enforcement officers. It also includes violent methods, such as threats to the target, and his/her family, for instance, showing them a picture of their children[18]. An increase in these actions has been seen mostly in Spain, Belgium, and the Netherlands. Regarding the Port of Rotterdam, in the Netherlands, it has been registered that corruption cases have sparked between 2003 and 2010.



Graph 3: Corruption and fraud investigations at Port of Rotterdam.[19]

Evidence shows that OCGs involved in trafficking cocaine are incredibly violent groups, but how do they corrupt, and why port employees participate in rip-off operations? Based on real-life justification, it needs to be considered that these justifications were made "after-the-fact rationalisations rather than before-the-fact neutralisations".[20] With this said, some of them referred to their previous history of gambling and drug abuse to highlight their precarious financial situation. Furthermore, others argued that they took part in living up to their family expectations, the fear of losing their families because they could not provide what they needed financially. Lastly, some of them became corrupt because they were "seduced" by way of life their colleagues were carrying by playing a role in the Rip-

[15] EMCDDA (n. 8), page 141.
[16] European Monitoring Centre for Drugs and Drug Addiction, 'Perspectives on Drugs, Cocaine Trafficking to Europe', Updated 31.5.2016, page 2.
[17] Ibid.
[18] Yarin Eski, Romano Buijt, 'Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam', 2019, page 373.
[19] Ibid; page 374-375.
[20] Ibid; page 207-208.

Off, the so-called "quick fix riches." These people who got involved in this *modus operandi* saw a possible way out of an inconvenient financial situation.[21]

The Rip-On/Rip-Off method has seen in the past years an increase in its use. However, nowadays, this method is less and less preferred because of the continuous robotisation of terminals; which does not give much space for OCGs to infiltrate. On the other hand, the excessive robotisation and regulation of just specific terminals might cause the water-bed effect, regulating more the security of a single port would mean that OCGs instead of shipping to that specific port would move their interests onto another, this would probably cause another port to be part of more Rip-on/Rip-off routes.[22] For this reason, it is crucial that steps towards automatisation are regulations are made as an overall cooperative action. Otherwise, they would become ineffective at a certain level.

Interestingly, contrary to the trend illustrated in *Graph 3*, Port of Rotterdam's efforts towards automation, digitisation, and digitalisation through projects such as PORTHOS, would result in fewer cases of corruption due to reduced workforce and dependence on autonomous vehicles for transport but may result in a significantly higher number of cyberattacks.

3.2. Container Seal

Container seal plays an important role when it comes to container security. Indeed, the global definition of container security stands within these words of the International Container Standard Organization (ICSO) which states that a container can be considered safe and secure when the cargo manifest matches the content of the container, which need to satisfy the requirements of the integrity of the container itself and the seal without any presence of third-party damage.[23]

This definition elucidates different aspects of container security. One of the aspects addressed in this report is the container seal's role in the maritime supply chain. The latter is paramount to determine if there has been a breach of container security.[24]

In 2014, IMO, the International Labour Organization (ILO) and the United Nations Economic Commission for Europe (UNECE) published the *Code of Practice for Packing of Cargo Transport Unit* in order to create a general code able to cover related container-issues. The document outlines every

[21] Yarin Eski, Romano Buijt, 'Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam', 2019, page 382-383.
[22] Frank Boerman Martin Grapendaal Fred Nieuwenhuis Ewout Stoffers, 'National Threat Assessment: Organized Crime', 2017, page 36-39.
[23] World shipping Council's definition, 2006; and Girish Gujar, Adolf K.Y. Ng, Zaili Yang 'Contemporary Container Security', 2018, page 10.
[24] Ibid; page 10.

aspect regarding the loading and closing of the container.[25] Analysing more deeply the previously mentioned code, chapter 11 "On completion of packing" comma 1 "Closing the Cargo Transport Unit (CTU)" shows the process of closing a shipping container.[26] Starting from the cargo packing of the CTU, once completed, the packer "should ensure that all closures are adequately engaged and secured".[27] Moreover, section 11.1.2 of the code states that, when required, the shipper should ensure that CTU, in international transport, has to be sealed with immediate action upon completion of the container packing procedure. It has to be closed with a seal carrying a unique identification number. Some countries may require that the number impressed on the seals meet the standard of ISO 17712.[28]

Section 11.3.3 of the Code of Practice for Packing of CTU clarifies that the party charged for packing the CTU should inform the shipper of the CTU's identification number. It can be either the container number or vehicle number, the Verified Gross Mass (VGM) of the unit, and the seal's identification number, to ensure that the identification numbers and the VGM are present in all transport documents (bill of lading, waybills, cargo manifests), which must be communicated to the carrier within the deadlines set by the latter.[29]

Once the container is packed and its doors closed, a high-security seal must be applied; besides, the seal number must be documented. In the scenario in which the shipper does not comply with this process, some shipping companies will seal the container upon cargo receipt.[30]

This supply chain security is subject to and must follow security seal standards. The leading standardised seal accreditation is ISO-7001. ISO is the International Organization for Standardization, a standard-setting body; its body consists of representatives from various national standards organisations.[31] As mentioned previously, the ISO 17712:2013 "establishes uniform procedures for the classification, acceptance, and withdrawal of mechanical freight container seals," it gives detailed information on seals that can be approved to be used in international commerce.[32] Container seals with ISO accreditation were born as a direct response to a massive security reform following the terrorist attacks on the United States of September 2001. Its final objective was to counter-terrorism,

[25] IMO/ILO/UNECE, 'Code of Practice for Packing of Cargo Transport Units (CTU Code)', 2014.
[26] Ibid; page 35.
[27] Ibid.
[28] ISO, 'ISO 17712:2013 (en) Freight Containers – Mechanical Seals' <https://www.iso.org/obp/ui/#iso:std:iso:17712:ed-2:v1:en> accessed August 16, 2020.
[29] Ibid; 'Code of Practice for Packing of Cargo Transport Units (CTU Code)', page 35-36.
[30] Maersk, 'Maersk Line Container Seal Policy', 2006.
[31] ISO, 'International Organization for Standardization' <https://www.iso.org/about-us.html> accessed September 3, 2020.
[32] Ibid; 'ISO 17712:2013 (en) Freight Containers – Mechanical Seals' <https://www.iso.org/obp/ui/#iso:std:iso:17712:ed-2:v1:en> accessed August 16, 2020.

illicit traffic, and smuggling of goods. ISO Norm 17712 aims at standardising the procedure to classify the acceptance and pick-up of a container.[33]

Image 3: Types of Container Seals, from the left: Klicker Bolt Seal, Bolt Seal, Cable Seal.

There are different types of container seals; among the most common, there are padlock seals, wire seals, and bolt seals; their final objective is to avoid tampering. With reference to the ISO 1772 seal classification, there are three classified types of security seals, based on the so-called barrier capacity or seal strength, and are as follows: "I" stands for Indicative, "S" stands for security and "H" for high security.[34] In order to remove a high-security seal (H), it is necessary to use professional lightweight tools, such as bolt croppers of high quality and cable cutters. Their impenetrability makes it impossible for third parties who want to open the container, to open it without clearly damaging the seal. U.S. trade partnership against terrorism (C-TPAT) requires "H" security seals. In 2012, the European Union and the United States of America signed a mutual agreement to recognise their respective programs AEO and C-TPAT. More common seal shapes are nail seals and cable seals. The seals used in container security chains differ from regular ones, known as "I" seals since they are subjected to mechanical tests before being classified as "H" seals.

Following ISO 17712 conformity (which classifies the seal as type H), the laboratory which should conduct the test must be certified based on ISO/IEC 17025 (General requirements for the competence of testing and calibration laboratories) and shall be accredited to perform testing specific to ISO 17712

[33] Ibid; Klicker Boalt Seal <https://www.megafortris.eu/product/klicker-container-bolt-seal/> consulted August 15, 2020; and High Security Container Boalt Seal, Fort Container seal <https://www.megafortris.eu/product/fort-container-seal/> consulted August 15, 2020.
[34] Ibid; and Cable Seal <https://www.megafortris.eu/product/mcl-350-cable-seal/> consulted August 15, 2020.

with these four tests: impact test, tensile test, bending test and cutting test.[35] Two certified laboratories are allowed to conduct mechanical tests on seals, which are: Mirdc and Dayton T. Brown. If a seal is bought from a supplier whose certification was not issued by one of these two laboratories, it means that the seal is not an "H" seal.

Bearing in mind that a container might have more than one seal since there are six different positions in which seals can be placed. Usually, if only one seal is applied, it supposedly goes on the right door' lock rods of the container since it is the first one to be opened while opening the container. Every seal carries an identification number, which is listed in the bill of lading.

The sealed container, if necessary, has to undergo a seal inspection to verify if there are any signs of tampering. Chapter 1.2.2 of the CTU Code highlighting the 'Safety' clarifies that the seal's identification number must match the cargo documentation. If it is not the case or shows clear signs of tampering, several further actions are necessary.[36]

Chapter 12 of the CTU Code, the section of "advice on receipt and unpacking of CTUs," comma 12.1 states that the consignee or the receiver of a CTU should check the unit's condition to see if there has been damage, a distortion, cracked or bent[37]. Furthermore, comma 2 gives instructions to check if the number on the seal matches the transport documentation number and if the seal is damaged or missing. If one of these scenarios occur, it would mean that the CTU has been opened during transport. In this case, the CTU operator "should be contacted" and aware of the current.[38]

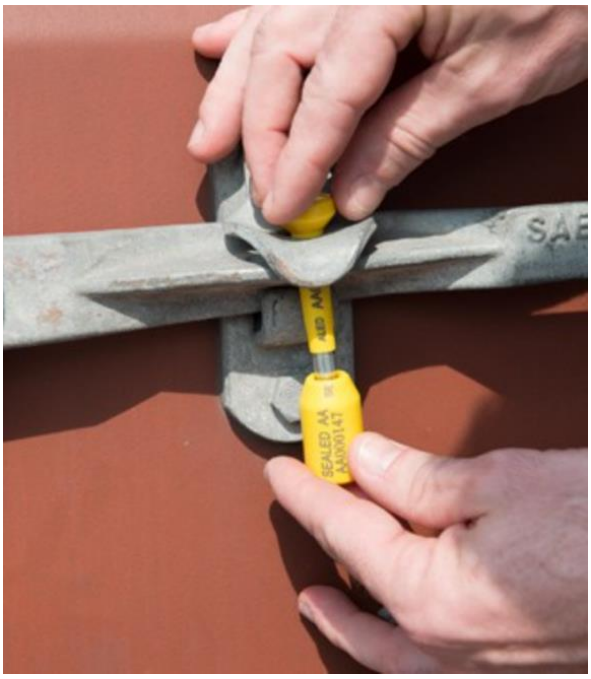


Image 4 Container sealed with a Bolt Seal

The seal is a bulwark when it comes to the security of a container supply chain. By acquiring information about its use and role, it gives the necessary tools and framework to further understand, in the next chapter, how drug cartels and smugglers try to bypass container seals with the Rip-on/Rip-off technique.

[35] Ibid; and 'ISO/IEC 17025:2017(en), 'General requirements for the competence of testing and calibration laboratories' <https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en:term:3.3> accessed August 16, 2020.
[36] Ibid. 'Code of Practice for Packing of Cargo Transport Units (CTU Code), 2014, page 2.
[37] Ibid; page 37-38.
[38] IMO et al., 'Code of Practice for Packing of Cargo Transport Units (CTU 3Code)', 2014.

3.3. The ISPS Code

Born as a reform to the 1974 SOLAS Convention, ISPS Code came into force on July 1, 2004.[39] This Code represents a legal security framework for ports, which is the primary international response to maritime security. It is currently used by 159 countries worldwide. However, this does not constitute a maximum-security regime, and within critical geographical areas, such as the Indian Ocean, no port facility adopted this set of rules.[40] Since the ISPS Code was born as a response to the 9/11 attacks, it guarantees more protection to the maritime sector. The purpose of the Code is to create a framework aimed at evaluating risks for the Governments to make changes where needed in terms of points of vulnerability for seaports infrastructures and to be able to adapt these security measures to different levels of threats. These uniformed measures, established by the Code, have to be implemented with a cooperation mechanism between all the actors involved in marine shipping: governments, port facilities, shipping companies.

The Code is divided into two sections, respectively A and B. Part A gives minimum mandatory requirements, addressed to ships and ports, and is "binding to contracting governments".[41] Meanwhile, while being more specific, Part B is mandatory and gives recommendations, and a set of guidelines addressed to the security assessments and plans. Part A outlines the principles of the Code, while part B gives specific indications on how to comply with such measures. When it comes to compliance with security measures such as security seals, the ISPS defines three levels of safety, which are defined as MARSEC, Maritime Security Levels:[42]

- MARSEC Level 1 is the basic level that port facilities and ships operate daily. It requires a seal check and other methods to prevent tampering.
- MARSEC Level 2 is a stricter level for a window of time in which a security risk becomes visible to security personnel.
- MARSEC Level 3 is an enhanced security measure for an imminent incident or one which has already occurred that must be kept for a defined time frame. These measures include preventing tampering.

However, the ISPS Code does not indicate which security seals need to be applied to containers to avoid tampering. Moreover, it does not specify the need for certified seals. On the other hand, the

[39]World Shipping Council, 'Industry Issues, Vessels and Ports' <http://www.worldshipping.org/industry-issues/security/vessels-and-ports> accessed August 18, 2020.
[40] Kenneth Christopher, 'Port Security Management – Second Edition', 2014, page 40.
[41] Ibid; page 59.
[42] United States Coast Guard, 'U.S. Coast Guard Maritime Security (MARSEC) levels' <https://www.uscg.mil/What-Is-MARSEC/> accessed August 17, 2020.

Customs-Trade Partnership Against Terrorism (CTPAT), another overlapping security initiative, states that the security seals that need to be used are ISO 17712:2013.

The WCO, in June 2009, saw the willingness of the 157 member nations to implement the Standards to Secure and Facilitate Global Trade Framework (SAFE Framework). China, Brazil, Japan, India, Chile, and the European Union considered implementing the security framework to implement programs. Many WCO members will need exceptional guidance and training in order to not only implement the framework but also to fulfil its final objectives.[43] Given the time-factor, the ISPS Code might now be considered obsolete because it comprehends all the tangible aspects of seaports' supply chain security. An aspect that needs to be highlighted is the relevance of electronic platforms in seaports for its supply chain to work and its security. The obsoletion of the ISPS Code and all the codes related to it show itself because the IT world itself and, more deeply, cyberattacks are slightly considered, it makes the global maritime industry highly unprepared for these types of attacks with a little legal framework to work.

The future challenges seaports security will tackle more "abstract" than "tangible"; for instance, a ship can be attacked by hackers by entering the IT system of the liner and might cause substantial damages. Every week 17 million cyberattacks are estimated.[44] Vessels do not need to be attacked directly, as it might happen with pirates, but an attack can be directed to the IT system of the shipping company and the Operational Technology System, quite easily. The IMO still has not formulated a regulation against cyberattacks and guidelines on cybersecurity. This deadlock can represent a significant open door for hackers. The ill-equipped maritime industry is extremely vulnerable.

These new-era challenges were brought to IMO by parties involved in maritime shipping; a step towards a safer environment was made in 2014 after the organisation consulted its member about a future maritime cybersecurity code and demanded insight on its content. In 2016, some cybersecurity guidelines were published; the framework developed was broad in its content; it resulted in being little practical to tackle attacks. Another step towards modernisation was made in 2017, IMO amended the ISPS and the ISM codes, giving guidelines on how seaports and operators should "undertake risk management processes".[45] These amendments will not enter into force until January 2021. The development of such practices and regulations are incredibly fundamental to protect the

[43] USAID, 'Customs Modernization Handbook, Authorized Economic Operators Program' <https://www.tfafacility.org/sites/default/files/case-studies/usaid_aeo_programs_handbook.pdf> 2010, accessed August 18, 2020.
[44] Vivian Louis Forbes, 'The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges', 2018, page 3.
[45] Ibid; page 4.

maritime security supply chain, even if they are cost-related, expensive, and a significant reform for the seaport system, which is in many cases.[46]

For instance, a cyberattack occurred in 2017 against Maersk shipping company. It suffered a ransomware attack called "Petya." The attack involved the company's container shipping. The oil tanker and tugboat were affected and crippled by computer outages. It resulted in a profit loss of 300million USD. It can be considered a financial disaster; some experts argued that this could have been avoidable using a blockchain system.[47] Shipping companies are becoming more concerned about the tools to fight cyberattacks. For this reason, some of them are developing a new system to face this issue with blockchain technology.

3.4. Container Tracking

Container tracking has become a more widely used component in the provision of container security, mostly due to the uncertainty of the shipping process. Tracking a container's exact location cannot be solved by just using a Global Positioning System (GPS) because there are four different logistic actors involved in a shipping "transaction" who do not have an existing cooperative tracking system.

The four different parties are defined as follows: First-party (1PL) It is a company that has produced goods and needs to export them via maritime shipping. There is the possibility that the 1PL might also be the goods' receiver. It is relevant for this party to track a container because the delay or "disruption" of the container might provoke a problem to "their supply chain."

The 1PL does not own the vessel nor the container. Otherwise, tracking would be facilitated; the liner owns both the vessel and containers. This scenario opens for a multi-tenancy issue for tracking. For instance, the goods are from the 1PL. However, a company or multiple own the ship, container, and truck. It is challenging for the 1PL to determine where to put a tracking device.[48]

The Second Party (2PL) "is a shipper or hauler," for instance, Maersk, Hapag-Lloyd, MSC. These shippers are the most active in tracking containers because they are liable if they do not fulfil the "contract" and deliver the container to the right destination. The liner owns the ships. However, not all of them own the containers placed in their cargo. In this scenario, 2PL would need to pay extra attention to manage the moment when the device is placed and eventually removed from the

[46] Ibid; page 5.
[47] IMO, 'Current Awareness Bulletin'. <http://www.imo.org/en/KnowledgeCentre/CurrentAwarenessBulletin/Documents/CAB%20248%20July%202017.pdf> 2017, accessed 19 August 2020; and Martyn Wingrove, 'Blockchain would have prevented Maersk cyber- attack' <https://www.rivieramm.com/news-content-hub/blockchain-would-have-prevented-maersk-cyber-attack-28063> 2017, accessed August 19, 2020.
[48] Link Labs, 'Container Tracking Systems: Everything you need to know', 2018 <https://www.link-labs.com/blog/container-tracking> accessed August 17, 2020.

container; given the vast number of containers present on board a vessel, it would be very time-consuming to do so.[49] Another aspect to take into consideration is that the 2PL does not hold much interest in doing so. Putting a tracking device is usually not included in the shipping contract unless it is the case of precious cargo. If it is the latter, 2PL will make an exception for tracking the container.

The Third Party (3PL) is a logistic provider, has the task to coordinate and schedule the shipping of goods for the 1PL "by using 2PL shippers".[50] The Fourth Party, 4PL, is an "independent body" that aids the 1PL "organise their supply chain across multiple third-party logistic providers. Given Faraday's law, it is almost useless to insert a GPS inside a container because since they are large metal boxes, they act as cages, so the wireless signal cannot get out of the metal box; the main reason why the 1PL should attach the GPS on the container's lock, so generally at the exterior.

Currently, on the market, the previously mentioned party can buy a tracking device; two of the most commons, concerning GPS based, are the locking mechanisms and the magnetic devices.[51] The locking mechanisms which has the goal to seal the container; they include a tracking device, and since they are placed within the sealing action, the 1PL is adding them. Another standard option is magnetic devices, which are positioned on the side of the container. They will not be placed on top of containers since shipping containers are stacked on top, so they are placed on a shipping container's structural rib. The device works with the accelerometer technique; in other words, it means that as soon as its sensor feels the ship moving, it turns on, "gets a GPS fix" via satellite or cellular.[52] Once the signal reaches the cellular constellation, the data transmitted, location, is sent and backend in the application provider's system and then "given" to the customer, in this case, 1PL.

There are both positive and negative aspects of container tracking. GPS container tracking systems are very meticulous, self-contained, and readily available.[53] Given the accuracy of such a system, there is no need for extra infrastructure to apply them on container shipping and the availability on the market (ORBCOMM)60, in which there are companies who make GPS exclusively for logistics. However, GPS tracking also bears some difficulties. Given the economic aspect, they are not cheap. It ranges for both GSM and GPS between $7 and $30 per month.[54]

Environmental conditions are part of the tracking's precision; for instance, there must be a clear view of the sky. As mentioned previously, shipping containers are stacked one on one, and if this is the case, it is almost impossible for the GPS to send a signal. The customer is only going to get a signal

[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Ibid.

once the container is placed somewhere else. Also, the GPS itself consumes a lot of battery, which usually needs to be replaced after six months, which means that the GPS cannot always be on since it would consume all the battery in just a few days.[55]

The GPS has to download from its satellite an ephemeris constellation data; thus, it will show its location. Nevertheless, to do so, it takes up to five minutes. Another way to track the shipping container is shorter-range wireless container tracking. This system does not work as GPS does; it does not send its data to a satellite or cellular. The system is malleable to a company's needs. (IoT) Internet of things.[56] Considering the economic aspect, compared to the less expensive GPS is around 7$ per container, this system costs per container $1 per month. Not only considering the "long investment" of the hardware product, a GPS application usually costs around $50-$300; meanwhile, for the shorter range is around $10.[57]

On the other hand, the battery of a GPS is power-hungry, so it will eventually die in a few months; the shorter-range wireless container tracking lasts much more. Since it is using Bluetooth technology, the battery could last up to three years or more. The difference standing between these two systems is that a GPS has to send the data to a satellite or cellular, turning it on and off and uploading a system. Meanwhile, the shorter-range using Bluetooth technology needs to transmit the signal to a "nearby.[58]

When it comes to this method's difficulties, bears are that it requires a much bigger infrastructure than GPS. The latter is "self-contained"; meanwhile, the shorter-range needs communication from the "tracking module to another part of the system." When it comes to moving a larger quantity of containers, this system can be worked out because some Bluetooth transmitter could be put just on some containers, "and then select a subset of those trackers to have their data backhauled via cellular"; with this method, the containers are being tracked, and fewer infrastructures are used.[59]

The difficulty also comes in the sense that it will need to backhaul the location data and "communicate that information" with the shorter range. However, if it considers the cost-benefit combination, it will be worth it at a certain scale point since it will offer lots of benefits compared to its costs. Given the complex scenario that shipping companies need to face when tracking a CTU, Maersk, and IBM

[55] Ibid.

[56] Port Technology, 'IoT standards for container connectivity launched' <https://www.porttechnology.org/news/iot-standards-for-container-connectivity-launched/> accessed August 17, 2020.

[57] Ibid. and 'Container Tracking Systems: Everything you need to know' <https://www.link-labs.com/blog/container-tracking> accessed August 17, 2020.

[58] Ibid.

[59] Ibid.

cooperated to create a Blockchain-based container tracking service, TradeLens. More than 20 port terminals have signed up for this program, including Port of Rotterdam (PoR) and PSA Singapore.[60]

4. Challenges head for seaports

4.1. Corruption at seaports

As mentioned previously, to tackle *modus operandi* such as the Rip-On/Rip-Off technique, policymakers, port authorities, and international maritime organisation should merge their will in order to create a legal framework when it comes to corruption at seaports, as well as implementing their security when it comes to being vulnerable towards cyberattacks and traceability. Given these premises in this chapter, it follows some policy recommendations that might be useful.

In the Rip-On/Rip-Off technique, a key factor for the operation's success are accomplices among seaports workers at the port of arrival and destination. Without them, OCGs would not obtain internal information, which is extremely useful for the outcome. To avoid or limit corrupted workers that could mine to the security of the seaport itself, the process to maintain a high level of security should start from the very beginning, at a job application stage. As outlined previously, various reasons contribute to port workers' corruption (history of gambling, financial issues, etc.). For this cause, when a candidate applies for a position inside the port, a background check should be conducted. Moreover, what should be dug deeper into is the financial status, history of drug abuse, gambling, and any other criminal records.[61] Furthermore, another security step to be conducted should be the screening of personnel who held key positions in handling containers. The reason behind the screening is their know-how, which is highly valuable to OCGs, to handle the container during the Rip-On. The screening of such personnel should be done by consulting logistic companies responsible for registering these employees and checking if any of them has registered any violations of occupational integrity.[62]

Employees who cover key position port authorities should reconsider who should have information and who should have access to it, a sort of balance of powers but with information, in a way in which information is compartmentalised, as a human blockchain, on a need-to-know basis.[63] Lastly, port authorities should implement and stimulate values such as integrity by delivering workshops for their employees with a security official and experts to explain the legal and penal outcomes of taking part

[60] IBM, 'Blockchain Industry Supply Chain' <https://www.ibm.com/blockchain/industries/supply-chain> accessed August 20, 2020.
[61] Yarin Eski, Romano Bujit, 'Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam' 2019, page 383.
[62] Ibid.
[63] Ibid.

in a Rip-On/Rip-off and its consequences. More in general, port authorities should enforce stricter access to their facility, such as surveillance tools, to prevent external parties which have an illegal business to have access to the docks and containers moreover to cooperate with policing authorities to share information on port employees which might be vulnerable subjects or at risk.

4.2. Blockchain Solutions

Blockchain has seen previously, will solve many issues that currently port facilities and more, in general, the international maritime traffic is facing, such as avoiding cyberattack, tracking containers and deeper the automatisation of ports. The global trade since 1956 uses a paper-based method for container shipping; everything that concerns the status of the containers and the cargo inside. This paper-based system makes the supply chain slower and too complicated given all the actors involved in the supply chain; for this reason, maritime security is put at stake by this obsolete method and gives a broad space for OCGs to carry out their illegal practice. The illusion of controls by organised crime is something that can be solved with blockchain. The automatisation of port thru blockchains would make for OCGs almost impossible techniques such as the Rip-on/Rip-Off.

Blockchain technology is a digital transaction ledger stored and maintained on multiple systems belonging to multiple entities sharing identical information; it creates a web that shares the responsibility of storing, maintaining, and, more importantly, validating the information present in the blockchain. The so-called authorised participants can review entries, and users can update information stored on the blockchain only if the network consensus algorithm validates it. Information stored in a blockchain can never be deleted and serves as a verifiable and accurate record of every transaction made within the ledger.[64]

Blockchain technology helps to make faster transactions, which are processed with few intermediaries with a peer-to-peer approach. Moreover, ledgers are updated automatically, and the transaction is executed, on both sides, at the same moment; it gives the blockchain a “fast transaction settlement”.[65] Another benefit for its users is the meagre cost, mainly because of the limited number of intermediaries, there is no “reconciliation work” required, and these transactions are validated by computing power and not a more expensive workforce.

The fundamental characteristic of this technology is its transparency. All the chronologies are stored in the ledgers; thus, there is a record of every transaction made. It is also an open-source technology,

[64] IBM, ‘IBM and Maersk demo: Cross-border supply chain solution on blockchain’ <https://www.youtube.com/watch?v=tdhpYQCWnCw> accessed September 5, 2020.

[65] Deloitte and Tax Consulting, ‘Continuous Interconnected Supply Chain Using Blockchain & Internet-of-Things in supply chain traceability’, 2017.

and all the transactions are visible to the authorised parties; furthermore, all accounts are identifiable. What makes blockchain technology a bulwark for the maritime supply chain is its reliability, which means that it does not have any single point of failure; the transactions made are irrevocable and immutable and registered in ledgers. The importance of blockchain technology in maritime shipping is broad. One of its most valuable points is that it reduces intermediaries, which translates into an increase in efficiency and reduction of costs.[66]

Taking a closer look at Blockchain technology's role in the maritime shipping supply chain and its benefits and risks that companies revolving around the maritime supply chain might have, it can be seen how without blockchain technology, there is a risk of a ripple effect. The cause behind this is an extended value chain. Companies face several risks with extensive supply chains since several actors are playing a role inside the chain (stakeholders, suppliers, distributors, customers).[67]

As a domino effect having an extensive supply chain might be ineffective in managing risks, making it difficult to predict and foresee risks to have a prompt and direct response. Another challenge that companies face with the obsoletion of the supply chain is the impossibility to see end-to-end. To track down and to have a 360-degree overview of the supply chain is extremely hard. Moreover, it is more comfortable to be exposed to risks such as tampering of containers, fraud, violation of conduct, and many more.[68]

The challenges facing today's supply chain are the amount of communication paperwork and the complex web of interactions between parties involved in this transaction, such as transportation providers, shipping industries, freight forwarders, customs, port authorities, and more. Born from the IBM and Maersk shipping company's idea, a new platform has been created designed to exchange event data and handle document workflows. What these two companies are doing is to apply blockchain technology in order to create a global tamper-proof system for digitising trade workflow and tracking shipments end-to-end. By doing so, the final objective is to eliminate frictions, among them point-to-point.[69]

This is a step forward for addressing the issues involved in tracking containers, which is with GPS technology system extremely expensive and applied just too few containers. On the other hand, with blockchain technology, there will be the potential ability to track down millions of containers each year at a smaller cost.

[66] Ibid.
[67] Ibid.
[68] Ibid.
[69] Ibid; and IBM, 'IBM and Maersk demo: Cross-border supply chain solution on blockchain'.

A recent example of how this technology works were carried out by the two companies to shipping flowers, a perishable good, from Kenya to Rotterdam in a container. With the current paper-based communication method, around 200 communications were issued; this leaves space for eventual issues with data accuracy presents on communications and data interpterion resulting in a higher increase of issues such as tampering. In simpler words, the communication process involved in shipping a container is intricated. Here follows, there will be an outline of how this process works using blockchain technology.

Image 5: An overview of the shipping process and its paper-based communication system.[70]

When the container leaves the port of origin, in this case, Mombasa, it requires the signature of three different agencies (KRA, KEPHIS, HCDA) moreover six more documents, which are packing list, commercial invoice, certificate of origins, phytosanitary certification, export license and bill of lading. This process is done in order for the export to be approved.[71]

The Kenyan farm submits a packing list that becomes visible to all the parties involved; this action starts a contract, which enforces an export approval workflow between the three agencies mentioned previously (KRA, KEPHIS, HCDA). Each agency has to sign the status, which is updated to everyone to simultaneously see information about the inspection of the flowers, the status of the container, and the trucker's pickup. The approval from customs is communicated to Mombasa's port, allowing them to prepare for the container. All actions relating to the documents and goods are captured and shared. Blockchain delivers a clear overview of all documents submitted when and by whom, where the

[70] Ibid; 'IBM and Maersk demo: Cross-border supply chain solution on blockchain'.
[71] Ibid.

flowers are, who owns them, and the next steps in their journey. Flowers are perishable, so there must be no delays or missed steps.

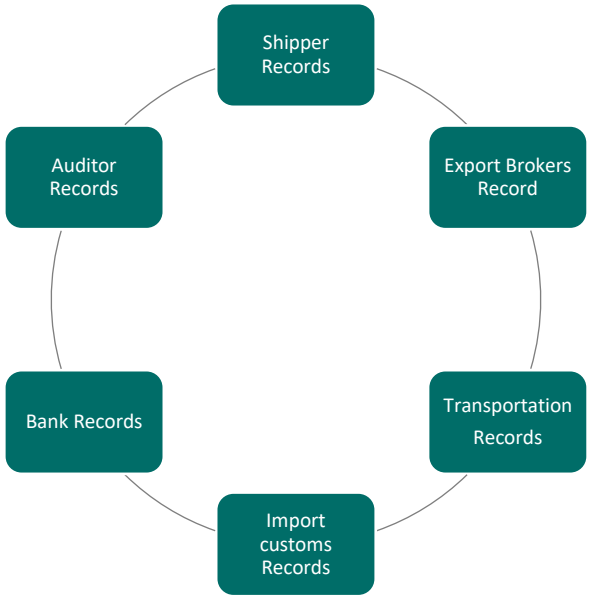


Image 6: An overview of the shipping process' communication system using blockchain technology.

Blockchain provides secure data exchange and a tamper-proof repository for these documents and shipping events. This system could significantly reduce delays and fraud, saving billions of dollars annually and, according to the WTO, reducing barriers within the international supply chain. It could increase worldwide GDP by almost 5% and total trade volume by 15%.

[72]

5. Conclusion

As outlined in this research, OCGs use the Rip-On and Rip-Off technique to introduce illegal goods inside a legit cargo; by doing so, they tamper with the container seals. This technique has a high percentage of success due to the few controls in place for container screening worldwide, at around 0.0005% of the total container volume. For this reason, it is tough for police enforcement to spot and find containers that have been used to fulfil such *modus operandi*.

Moreover, container seals tampering becomes facilitated when the number of containers is almost overwhelming in ports because it is hard for port authorities and police enforcement to spot which containers have been tampered with. Container seals show signs of tampering when they are broken or replaced with a different serial number.

Such practices give authorities a much broader area in which they need to look at by doing a risk assessment on a small number of containers; furthermore, it has been seen how introducing blockchain technology could solve some problems involving container security. It would be easier for law enforcement to collect all the data needed for risk assessment, having a beginning-to-end

[72] Ibid; 'IBM and Maersk demo: Cross-border supply chain solution on blockchain'.

traceability of the container and its routes, to tackle frauds and improve Customs compliances and trade facilitation.[73] Currently, IMO, UNODC, and WCO monitor how this tool can ensure a global safer supply chain crime proof.

The fundamental role blockchain will have in the near future is to improve security in seaports worldwide, concerning techniques such as the Rip-on and Rip-Off and cyberattacks, a new challenge maritime security has to face. It will also speed the process of ports automatisation, in order to make not only the maritime supply chain more efficient in terms of speed, economic costs, and time but also to avoid any container tampering during the whole process by giving to every party involved in the supply chain all the information regarding the status of the container. Blockchain technology shows itself to be one of the keys to container security and maritime security in general, asking for the maritime community to speed the IT process for long-term results and to safer seaports. It will be the *conditio sine qua non* to the enforcement of port security.

[73] United Nations Office on Drugs and Crime, 'Container Control Program, 2019 report' page 20.

6. Bibliography

6.1. Literature

Girish Gujar, Adolf K.Y. Ng, Zaili Yang *'Contemporary Container Security'*, 2018.

H.J.M. Staring, L.C.J. Bisschop, R.A. Roks, E.G. Brein and H.G. van de Bunt, *'Drug Crime in the Port of Rotterdam: about the phenomenon and its approach',* 2019.

Ajatshartu Bhattacharya and Benjamin Peters, '*The Underwater War on Drugs: An overview of the Dutch Customs Diving Team'*, 2020, Invictus Corporation Ltd., August 2020.

Kenneth Christopher, '*Port Security Management – Second Edition'*, 2014.

Vivian Louis Forbes, '*The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges*', 2018.

Yarin Eski, Romano Buijt, *'Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam*', article consulted November 5, 2020.

6.2. Reports

Deloitte and Tax Consulting, '*Continuous Interconnected Supply Chain Using Blockchain & Internet-of-Things in supply chain traceability*', 2017.

European Monitoring Centre for Drugs and Drug Addiction, '*Perspectives on Drugs, Cocaine Trafficking to Europe'*, Updated 31.5.2016.

EUROPOL, '*EU Drug Markets Report – a Strategic Analysis*', 2019.

Eurostat*, 'Gross weight of seaborne freight handled in all ports'*, 2018 <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Gross_weight_of_seaborne_freight_handled_in_all_ports,_2018_(tonnes_per_inhabitant).png> accessed September 1, 2020.

Frank Boerman Martin Grapendaal Fred Nieuwenhuis Ewout Stoffers, 'National Threat Assessment: Organized Crime', 2017.

IMO, '*Current Awareness Bulletin'* <http://www.imo.org/en/KnowledgeCentre/CurrentAwarenessBulletin/Documents/CAB%20248%20July%202017.pdf> 2017, accessed August 19, 2020.

Maersk, '*Maersk Line Container Seal Policy'*, Report 2006.

United Nations Conference on Trade and Development, *'Review on Maritime Transport 2018'*, 2018.

United Nations Office on Drugs and Crime, *'Container Control Program, 2019 report*' 2019.

6.3. Legislation and cases

IMO, '*Safe Transport of Containers'*, <http://www.imo.org/en/MediaCentre/HotTopics/container/Pages/default.aspx> accessed August 15, 2020.

IMO/ILO/UNECE, '*Code of Practice for Packing of Cargo Transport Units (CTU Code)',* 2014.

ISO, '*ISO 17712:2013 (en) Freight Containers – Mechanical Seals'.* <https://www.iso.org/obp/ui/#iso:std:iso:17712:ed-2:v1:en> accessed August 16, 2020.

ISO/IEC 17025:2017(en), '*General requirements for the competence of testing and calibration laboratories*', <https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en:term:3.3> accessed August 16, 2020.

United States Coast Guard, '*U.S. Coast Guard Maritime Security (MARSEC) levels'*, <https://www.uscg.mil/What-Is-MARSEC/> accessed August 17, 2020.

USAID, '*Customs Modernization Handbook, Authorised Economic Operators Program',* <https://www.tfafacility.org/sites/default/files/case- studies/usaid_aeo_programs_handbook.pdf> 2010, accessed August 18, 2020.

World Shipping Council, '*Industry Issues, Vessels and Ports'* <http://www.worldshipping.org/industry-issues/security/vessels-and-ports> accessed August 18, 2020.

6.4. Secondary Sources

Cable Seal, <https://www.megafortris.eu/product/mcl-350-cable-seal/> consulted August 15, 2020.

European Monitoring Center for Drugs and Drug Addiction, '*Interactive map of cocaine trafficking routes to Europe'* <https://www.emcdda.europa.eu/cocaine-trafficking-europe_en> accessed September 1, 2020.

High Security Container Boalt Seal, Fort Container seal <https://www.megafortris.eu/product/fort-container-seal/>consulted August 15, 2020.

<https://www.rivieramm.com/news-content-hub/blockchain-would-have-prevented-maersk-cyber-attack-28063>, 2017, accessed August 19, 2020.

IBM, *'Blockchain industry supply chain'* <https://www.ibm.com/blockchain/industries/supply-chain>, accessed August 20, 2020.

IBM, '*IBM and Maersk demo: Cross-border supply chain solution on blockchain'* <https://www.youtube.com/watch?v=tdhpYQCWnCw> accessed September 5, 2020.

ISO, *'International Organization for Standardization',* <https://www.iso.org/about-us.html> accessed September 3, 2020.

Klicker Boalt Seal, <https://www.megafortris.eu/product/klicker-container-bolt-seal/> consulted August 15, 2020.

Link Labs, '*Container Tracking Systems: Everything you need to know*', <https://www.link-labs.com/blog/container-tracking> accessed August 17, 2020.

Martyn Wingrove, '*Blockchain would have prevented Maersk cyber-attack*'

Port Technology, *'IoT standards for container connectivity launched'* <https://www.porttechnology.org/news/iot-standards-for-container-connectivity-launched/> accessed August 17, 2020.

United Nations Office On Drugs and Crime, '*CCP Glossary of Terms'* <https://www.unodc.org/ropan/en/BorderControl/container-control/ccp-glossary-of-terms.html> accessed August 25, 2020.

6.5. List of Figures

Graph 1: All Cargo (Crude Oil, petroleum products, and gas; main bulks; other dry cargo)

United Nations Conference on Trade and Development, based on data supplied by reporting countries and as published on government and port industry websites, and by specialist sources. Notes: Dry cargo data for 2006 onwards were revised and updated to reflect improved reporting, including more recent figures and a better breakdown by cargo type. Since 2006, the breakdown of dry cargo into main bulks and dry cargo other than main bulks is based on various issues of the Shipping Review and Outlook, produced by Clarksons Research. Total estimates of seaborne trade figures for 2017 are based on preliminary data or the last year for which data were available.

Graph 2: Gross weight (tonnes per inhabitant) of seaborne freight handled in all seaports (2018)

Eurostat, 'Gross weight of seaborne freight handled in all ports', 2018, accessed September 1, 2020.

Image 1: Cocaine trafficking routes to the EU

European Monitoring Center for Drugs and Drug Addiction, 'Interactive map of cocaine trafficking routes to Europe' <https://www.emcdda.europa.eu/cocaine-trafficking-europe_en> accessed September 1, 2020.

Image 2: An overview of the Rip-On/Rip-Off *modus operandi*

H.J.M. Staring, L.C.J. Bisschop, R.A. Roks, E.G. Brein and H.G. van de Bunt, 'Drug Crime in the Port of Rotterdam: about the phenomenon and its approach', 2019 page 23.

Graph 3: Corruption and fraud investigations at Port of Rotterdam

Yarin Eski, Romano Buijt, 'Dockers in Drugs: Policing the Illegal Drug Trade and Port Employee Corruption in the Port of Rotterdam', 2019, page 374-375.

Image 3: Types of Container Seals, from the left: Klicker Bolt Seal, Bolt Seal, Cable Seal

Klicker Boalt Seal <https://www.megafortris.eu/product/klicker-container-bolt-seal/> consulted August 15, 2020; and High Security Container Boalt Seal, Fort Container seal <https://www.megafortris.eu/product/fort-container-seal/> consulted August 15, 2020. Cable Seal <https://www.megafortris.eu/product/mcl-350-cable-seal/> consulted August 15, 2020.

Image 4: Container sealed with a Bolt Seal

IMO/ILO/UNECE, 'Code of Practice for Packing of Cargo Transport Units (CTU 3Code)', 2014.

Image 5: An overview of the shipping process and its paper-based communication method

IBM, 'IBM and Maersk demo: Cross-border supply chain solution on blockchain' <https://www.youtube.com/watch?v=tdhpYQCWnCw> accessed September 5, 2020.

Image 6: An Overview of the shipping process' communication system using blockchain technology

IBM, 'IBM and Maersk demo: Cross-border supply chain solution on blockchain' <https://www.youtube.com/watch?v=tdhpYQCWnCw> accessed September 5, 2020.