ERASMUS UNIVERSITY ROTTERDAM

Erasmus School of Economics

Bachelor Thesis Urban, Port, and Transport Economics

What makes a port vulnerable to cyber risks?

Name student: Sepp Dijkers

Student ID number: 532984

Supervisor: A.W. Veenstra

Second assessor: M. Jansen

Date final version: 05-07-2022

Abstract

Recent years have seen a surge in technological dependence the maritime world. This has brought automatization and efficiency benefits in ports, but also opened the door to new risks and vulnerabilities. Being cyber vulnerable is a broad concept, which depends on both awareness within the port and sufficient technological security. This paper makes use of financial data and port characteristics to determine what seems to be the most targeted aspects regarding cyber vulnerability in the port landscape. First, theoretical groundwork for the report will be laid out using recent literature on cyber technology and cybercrime. Then, data sources and methodology for the empirical analysis will be illustrated. Using this methodology this report will analyse how certain port characteristics are related to cyber vulnerability, defined by economic size. Finally, this paper will try to conclude what makes a port cyber vulnerable using the results from the analysis, leaving remarks for further discussion.

Table of Contents

ABSTRACT **2**
INTRODUCTION **5**
LITERATURE REVIEW **6**
Introduction 6
Finding literature 6
Digitization of the maritime world 6
The risks of over-reliance 7
Becoming cyber secure 7
A DEFINITION OF CYBER VULNERABILITY **10**
Introduction 10
Cyber vulnerability in practice 10
Cyber vulnerability in financial terms 10
Cyber vulnerability in this report 11
METHODOLOGY & DATA **12**
Introduction 12
Methodology of the research 12
Data sources and usage 13
The research question 15
I. DOES CONNECTIVITY AFFECT CYBER VULNERABILITY IN PORTS? **16**
Introduction 16
Does more connected mean more vulnerable? 16
Results from Data 17
Conclusion 17
II. DOES MAIN GOODS TYPE AFFECT CYBER VULNERABILITY IN PORTS? **18**
Introduction 18
Does goods type matter? 18
Results from Data 18
Conclusion 20
III. DOES GEOGRAPHIC REGION AFFECT CYBER VULNERABILITY IN PORTS? **21**
Introduction 21
Cyber criminals in different world regions 21
Results from data 21
Conclusion 24
SUMMARY OF RESULTS **26**
Introduction 26
Results 26
Assumptions & Constraints 27
CONCLUSIONS & DISCUSSIONS **28**

INTRODUCTION 28
CONCLUSIONS 28
DISCUSSIONS 29
APPENDIX 30
APPENDIX A.1.: LIST OF ALL PORTS REGISTERED IN LLOYD'S LIST ONE HUNDRED PORTS (2021) 30
APPENDIX A.2.: VARIABLE NAMES AND EXPLANATION 32
APPENDIX A.3.: OLS REGRESSION SHOWCASING RELATIONSHIP BETWEEN DEPENDENT VARIABLE 2019 ANNUAL TEU THROUGHPUT (IN MILLIONS) AND ALL INDEPENDENT VARIABLES TESTED FOR IN THIS PAPER. 34
REFERENCES 35

Introduction

Recent years have seen a surge in technological and cyber systems prominence in ports all over the world. This has led to efficiency gains, benefits in communication, and sustainability benefits (DNV, n.d.), all in line with the statements set out that the pandemic has accelerated the already high levels of digitalization in the maritime sector (UNCTAD, 2021). The flip side to this however, is that a heightened dependability on technological software and systems leads to a much higher risk of cyber criminals interfering with these systems. An article from Le journal de la Marine Marchande (2020) highlighted this issue, stating that cyber-attack numbers had increased by 400% over the preceding period, as researched by maritime cyber security company Naval Dome. This only further highlights the growing importance of cyber security within the maritime landscape, seeing as a call for digitization will keep the reliance of ports on digitized systems growing.

Up until now, the relationship between cyber-attacks and ports has not been researched in great numbers, which is why this report will try to add to existing literature. The issue seems to be driven by the need of new systems and technologies will often need time to get accustomed to. Together with the need for keeping employees in the port well informed regarding cyber security and on the other side keeping systems up to date is a balance which is hard to accomplish, especially since cyber security is something for which it is yet unclear what gives you the best “bang for your buck” (Ducaru, 2016). This makes it interesting to see how ports invest into both of these factors, and if this is something which differs per region, port type (container port, bulk port), or economic size of a port. This paper will look into these effects using three sub questions, and ultimately hoping to answer what role they play in the cyber vulnerability of a port.

Literature Review

Introduction

This chapter will lay a focus on the theoretical groundwork surrounding cyber vulnerability. Ranging from literature on technological developments in maritime industry to how theory and interviews state that companies in the maritime world try to prevent cybercrime and cyber risks. This literature will serve as a background understanding, which will link to the results found in the later chapters containing sub-questions and empirical analysis.

Finding literature

To find the literature relevant to this report, I made the most use of the key words “cyber security”, “cyber vulnerability” and “cybercrime”. My first goal was to find articles written aimed at the maritime world by adding key words phrases like “in ports” or “in the maritime world”, if there was no literature of interest, I looked at articles covering the beforementioned topics in general. To gain more insights on the role of port characteristics with regards to cyber vulnerability I added key phrases like “in relation to location”, “with regards to connectivity” and “based on goods type”. When deciding what type of literature to use, I opted for a combination of articles published on respectable websites and often cited academic papers. Reading this literature, I focused mainly on the abstract, headers and conclusion to determine if it was of interest. If that was the case, I took a more in depth look into the chapters that contained useful information, retrieving mostly opinions of people who researched the topic or the ideas on how companies should adapt to the new landscape.

Digitization of the maritime world

The maritime world has seen developments in many of its sectors, seeing the creation of a more efficient and connected network (Donepudi, 2014). Donepudi states that the maritime industry has been keen on advancing on a technological front in recent years. He sees the ultimate goal of a port as that of becoming a smart operating hub, where human processes are supported by the most suitable digital assistance, creating safer, more accurate and more competitive centres of maritime trade. Besides the benefits of digitization, which seem to attract many of the stakeholders, even those who are less keen on the growth of technological influence seem to no longer have another choice. As stated by Balcombe et al. (2019), shipping will have little to no chance in meeting climate goals set out to reach a 50% greenhouse gas reduction by 2050 if it does not adapt to more efficient technological processes or new transport methods.

He states that to forge shipping in a sustainable industry for the coming decades, a combination of fierce technological implementation, complimented by the use of new fuel types and supporting international and national policies is required.

The risks of over-reliance

The push towards a more digitized port thus seems uncontested. But this digitization leads to a reliance on this technology to function successfully in order for it to work as efficiently as it promises to do. In recent years, ports all around the world have seen outages and disruptions instigated by cyber criminals, benefiting from the reliance these operators now have on technology.

CSIS (2022) highlights three of the major cases of these cyber-attacks happening in the maritime sector, placed on a list of what they regarded as very impactful cyber-attacks which happened since 2006. Some examples of these major attacks concerning ports where those of an operations hack in 2020 targeting the port of Iran, an interception of password information by hackers in the port of Houston, Texas in September 2021 and attacks on the transport network of the port of Durban in 2021. Smaller scale cyber-attacks happen in ports around 10-12 times a day, highlighting the prominence of the issue, as stated by the Union des Ports de France (Stormshield, 2021)

Akpan et al. (2022) further broaden this issue by illustrating that the maritime world in particular faces a high risk of being vulnerable to such attacks, because every node of the transport chain within it has a chance of being intercepted. Much of the weakness, as they state, comes from the fact that critical infrastructure of the port transport chain is not adequately protected. Fallouts in this infrastructure quickly leads to big consequences for the rest of the chain. Something which then is quite remarkable when looking at what the reasoning behind these cyber criminals and they target is, is that it is often not the main goal to target the port to hide data or keep a drug transport secret (Stash Kempinski, 2021). It seems the port is mostly targeted to disrupt the network it provides, causing transport issues or shutdowns that hinder the ports and thus forcing the port to pay out the hackers the ransoms they demand, an issue which seems more and more apparent in all supply chain companies (Rivero, 2022).

Becoming cyber secure

To combat this increasing risk of having disrupted infrastructure as a consequence of cyber disruptions, the port needs to find a way to increase its cyber awareness and decrease its cyber vulnerability. The two main factors which come back in literature as main factors of combatting this vulnerability are cyber awareness, based on the human aspect of knowing when you bring the port at risk of being cyber vulnerable, and replacement of old systems, which are replaced by more up to date cyber systems.

But, finding an optimal balance in investing in human solutions and IT solutions is something which seems to have caused issues in the maritime sector (Ducaru, 2016). Much of the reason that this balance is so hard to find, as Ducaru explains, is because cyber security in itself is something which is a very new phenomenon in most industries, the maritime sector included. If either too much is spent on the human side of the spectrum and little on the technological side, the security systems may not be able to protect you from the attacks, how good informed your employees may be. The other way around also seems to yield inefficient results. Keeping up with a threat as quickly changing as these cyber-attacks, due to the implementation of new technologies and changing systems, makes the issue of finding this balance very important, but difficult and unpredictable as well (Ducaru).

Tam & Jones (2018) feel as though the current cyber policy perspective is not sufficient, and should be looked at with a different approach. They do this by splitting up the human and technological aspects into two investments in different time periods. In the short term, by increasing awareness on the issue that they find is lacking a lot currently and, on the longer term, a switch to newer systems which offer better protection against the cybercrimes.

Tam & Jones illustrate that the way to create a more cyber secure maritime landscape, is to make use of policies which motivate the port companies to follow the short and long terms goals in changing their approach to cyber security. Using knowledge from previous attacks and probable future attacks to have the right system and awareness to handle each issue as efficiently as possible.

Saini et al, (2012) take a broad look at all aspects of cyber security. Ranking the criminals that operate in this world from small to the highest level, what types of crimes are often seen and looking at how companies can react to the threat's cybercrime poses. They propose companies can follow the "market value approach" for investments in cyber vulnerability, where a company looks at the value it would lose if it would be shut down for a period of time due to a cyber-attack, and bases the investment on that number. Besides the approach they urge that countries look at the security they have on a national level, as a weak framework on a national scale seems to attract and motivate cyber acts within the country.

Adding to this, another issue which currently causes more inefficient targeting of cyber-attacks and vulnerability initiatives is explained by Stash Kempinski, 2021. Namely, most cybercrimes across industries are not properly reported to the correct authorities.

This means that creating an overview and being able to see which type of attack causes the most problems, becomes an issue, as seen in the fact that reports to the Operational Technology Cyber Attack Database (OTCAD) saw over one third of the reports labelled as having a missing cyber-attack type identification.

Most of the reasoning behind this is that cyber-attacks are seen as bad publicity, advertising that the port or company is susceptible to such an issue, which is why they rather not disclose it (Kempinski, 2021). Linking this to the plans laid out by Tam & Jones (2018) to use data to prepare for coming attacks, may be a cause for concern if the data needed to do so is not available.

A definition of cyber vulnerability

Introduction

This chapter will illustrate the main construct for this report, cyber vulnerability. Much like the earlier chapter on theoretical background, this chapter will have a theoretical framework in which it uses interviews held with industry specialist and statements made by the top maritime companies to show their opinions on cyber vulnerability. Then, it will make use of the financial statements, to decipher what the companies in the dataset deem as cyber vulnerability. Defining if this is seen as a more software heavy investment, or more human sided.

Cyber vulnerability in practice

Recent cyber-attack cases have made it so the companies operating at the highest level within the maritime world have had to deal with new unprecedented challenges. Maersk (2020) saw that their approach to security had to change following a system shutdown in 2017. Adam Banks, CIO of Maersk stated after the 2017 attacks that: "Cyber-attacks are not going to go away and technology is becoming a more strategic asset in the future of our business", which he underlined by saying that Maersk would continue building on its IT systems and raise awareness to its employees for cyber security. FERM, a collaboration between among others the Dutch government and Port of Rotterdam sees cyber resilience, as they call it, as an integral part of the maritime landscape, stating: "It is of importance to us all. Small and big businesses. Often, it's not about enormous amounts with phishing emails and CEO fraud, but it can very well become expensive. Especially when added up." They hope to create a network for cyber security. Combining experience with the ability to learn from each other and stress the importance of becoming aware of cyber vulnerability and the company's own protection systems (FERM, 2016).

Cyber vulnerability in financial terms

When reporting in their yearbooks most port companies illustrated spendings on cyber initiatives as either software additions or cost attributed to increases in intangible fixed assets. Cyber awareness was not listed as an independent cost factor, listed as a segment of goodwill and thus hard to be traced back into financial terms. This leads to interpretation of software as main reference point. Which does not paint a full picture, as implementing software in larger quantities does not mean the company is better protected (Harvard Business Review, 2018). This because criminals will often find a path of least resistance, searching for an area of IT which is less sophisticated than the rest, an absence of proper management and awareness thus leads to inefficiencies even when spending a lot into software.

Businesses still opt for large investments in software because they are something which can be easily managed and aligned with business needs, where awareness is less so (Harvard Business Review). This thought is underlined by cyber risk & resilience company McKinsey & Company's 2019 report on perspectives on transforming cybersecurity, which states that their research showed that mores spending did not correlate directly to higher protection, as without management this spending was often put in the wrong areas. However, they further highlight that spending a bigger portion of expenses on IT renewal and security does guarantee a higher level of protection to cyber vulnerability overall, regardless of the level of cyber awareness and ability of the company's employees (McKinsey & Company, 2019). The relationship found in the dataset's yearbooks between cyber expenditures and economic size is reflected in Figure 1 below, signifying a positive linear relationship.

Figure 1: Scatter graph between 2019 annual TEU throughput and cyber expenditures.

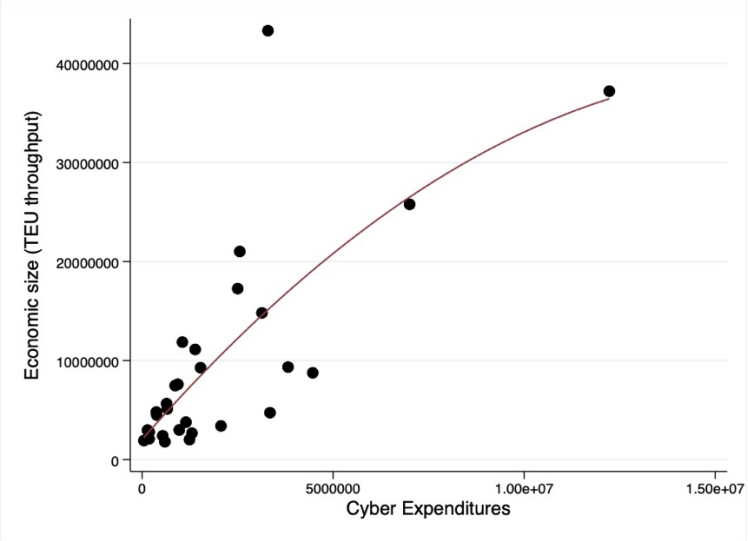

Figure notes: Figure depicts relationship between cyber expenditures and annual throughput measured in TEU in 2019 for a port, with quadratic trendline.

Cyber vulnerability in this report

The previous segments last statement allows for the rough interpretation that a company who spends more on software is more concerned regarding cyber vulnerability, an assumption that must be made as cyber awareness is hard to allocate to financial terms. This hard to connect relationship between expenditures and vulnerability is why this report will make use of economic size as a measure for vulnerability, based on the interpretation that a bigger economic port will showcase more prominence on world markets and in turn be more susceptible to national and international threats.

Methodology & Data

Introduction

Following the theoretical background, this chapter will focus more on how the empirical analysis in the coming chapters will be shaped. First it will explain how the regressions and tables will be shaped, looking at how the results found in research will be presented in the report. After having given a general picture of the research methodology, data used will be listed, along with its sources. This to give a clearer picture as to what brings the report to its results.

Methodology of the research

The previous chapter laid out the definition of the main construct for the report stating what is: *"A definition of cyber vulnerability".* Making use of theory combined with yearly reports published by the ports, the latter further highlighted in the data sources. This chapter defined what ports see as a cyber risk by looking how their investments relate to more cyber vulnerability.

Making use of this groundwork, this report will use of three sub-questions which all cover a defining characteristic of a port. If the answer is known as to which effect a certain characteristic has on the level of cyber vulnerability, it allows for an answer as to what affects a port's cyber vulnerability as a whole. The three sub-questions will all utilize Ordinary Least Squares (OLS) regressions. They are listed as follows:

- ***Does connectivity affect cyber vulnerability in ports?***
  The first sub-question of the three, *"Does connectivity affect cyber vulnerability in ports?"*, will make use of the comparison between the dependent variable cyber vulnerability, which was defined as the economic size of the port in the previous chapter, and the ports connectivity as independent variable. This connectivity is determined by the amount of direct port connections a specific port has. That way, it will try to determine the effect a ports international connectivity plays a role in the vulnerability it has to cyber risks.

- ***Does main goods type affect cyber vulnerability in ports?***
  The following chapter *"Does main goods type affect cyber vulnerability in ports?"* will make use of a similar OLS regression, making use of the same dependent variable, with a difference being that this time the independent variable will be the main goods type the port has as throughput. This will then result in spending on cyber vulnerability illustrated by economic size being weighed off against the different goods types, created as dummies.

The dummy categories being as follows, as stated in UNCTAD (2021): container port, liquid bulk port and dry bulk port. Other goods type ports, like Roll-on Roll-off ports and ports specialized in unique products, also mentioned in the UNCTAD list, will be listed if applicable, but this only applies for more rare situations where a port is dedicated to non-container or bulk goods. As a result, each good type will have a value attributed to it highlighting whether exporting a different type of good affects the port's cyber vulnerability.

- ***Does geographic region affect cyber vulnerability in ports?***
  The final of the three sub-questions containing OLS regressions will do so much like the one before it. In this sub-question: *"Does geographic region affect cyber vulnerability in ports?"*, the dependent variable remains the same, representing the ports cyber vulnerability. The independent variable here does not focus on the goods type being exported however, but centres around the geographic region in which the port resides. Two OLS regressions will be run, one using these dummies on a continental scale, and one on a more specific scale, as specified in Lloyds List 's *One Hundred Ports 2021* (2021). This will make for dummies for each continental region: Europe, Asia, North America, South America, Africa, Oceania, and for dummies more specified within this region, ranging from North-western Europe and the Mediterranean area to the Middle East.

Data sources and usage

To carry out these regressions and correlations, it is important to draw this information from a dataset with all information needed. The dataset used for this report will consist of the hundred ports listed in Lloyds List 's *One Hundred Ports 2021* (2021), as these will be of such a scale that accessible and international yearly reports will be published on their website in a very thorough fashion. A list of all the ports listed in this article can be found in Appendix A.1. Some examples of these yearly reports being the annual reports of the PSA International (2020) and Qinhuangdao Port (2020).

All yearly reports used in the dataset will be of the year 2019. The choice for this year was based on the fact that it was the last year which did not showcase disruptions in the maritime industry due to the Covid pandemic, which may lead to unreliable results or unnatural choices made by some of the port authorities. These anomalies can be seen in the article on maritime mobility published by Millefiori et al. (2021), in which oil prices dropped and maritime trade worldwide saw unexpected decreases, disrupting the port landscape for 2020 and most of 2021. Because the 2019 annual reports will be used, any foreign values published in reports will be exchanged to dollars with the use of exchange rates of late 2019, using data regarding these rates obtained from OANDA (n.d.).

To determine the connectivity for the ports in the dataset, UNCTAD's 2020 article covering the *world's top 50 container ports by degree* is used. This article lists all direct connections a port has to other ports for the top 50 ports by this metric in the world. If this number is low, it means that a port has to often have goods transhipped from other nearby ports instead of a direct line (UNCTAD, 2020). Many of the ports on this list are also found on Lloyds list's *One Hundred Ports 2021* list, allowing for comparisons.

Lloyd's List (2021) provides the TEU throughput for all ports on the list for both the years 2019 and 2020. This will allow for a clear overview of economic size. Much like the earlier variables these numbers are for 2019 to avoid the Covid shock in the years after it.

To gather data on the geographic region and main goods type exported as needed to obtain results for the last two sub-questions *"Does main goods type affect cyber vulnerability in ports?"* and *"Does geographic region affect cyber vulnerability in ports?"*, data from Lloyd's List of the one hundred biggest ports (2021) will also be used. Namely, besides stating TEU outputs of the years 2019 and 2020, the list states in which region a port is located, and gives information on what number of terminals and impact the port has on its region surrounding it. Combining this data with the dependent variable of economic size published on Lloyd's List will allow for the creation of dummies to be used in regressions. Additional sources for finding goods types are UNCTAD (2021) and Marine Traffic (n.d.), the first one summarizing year-end statistics and the latter showcasing recent trends in port call goods types.

An overview of all variable names and their corresponding meanings and values can be found in the Appendix A.2. table, together with an explanation as to how the variable has been measured and in what a value means of the variable. Figure 2 below shows the placement of the ports used in this paper on a world map.

Figure 2: World map with 100 ports listed in Lloyd's List 2021.

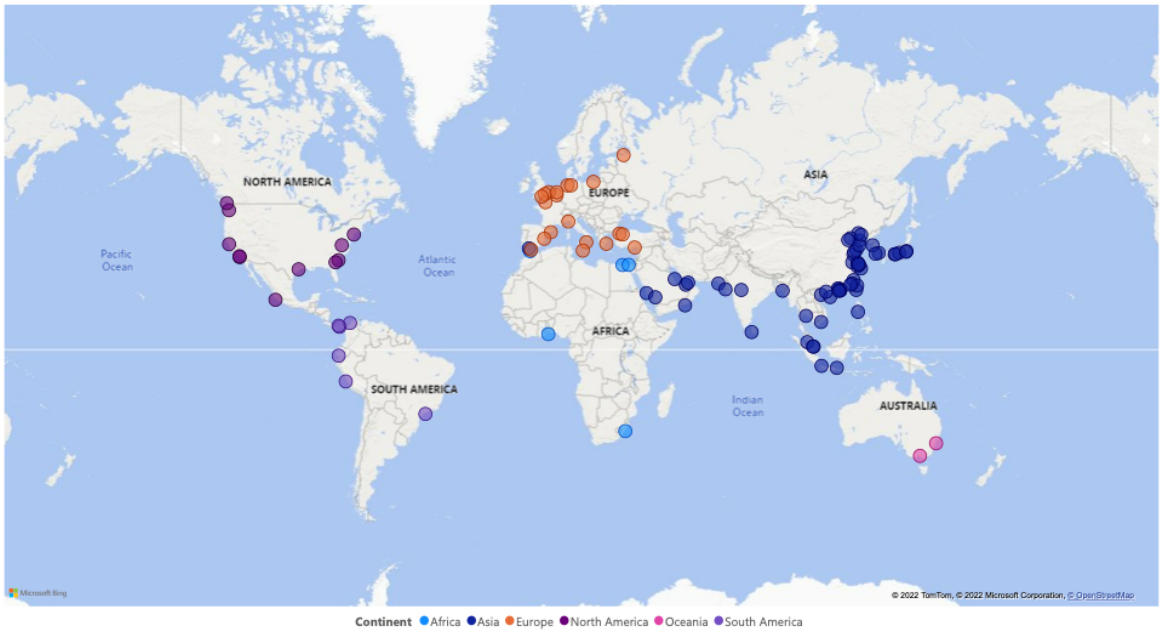

Figure Notes: World map showcasing all port locations of ports listed in Lloyd's list *One Hundred Ports* (2021). Ports categorized per world continental region. Map retrieved from TomTom (2022).

The research question

Literature shows the struggle between becoming more involved with cyber systems and dealing with the risks it brings. Some insights are made regarding which aspects are determining for how much a company decides to spend into cyber expenses and how vulnerable a port seems to be in cybercrime aspects. Whether this is based on the company size, where it is located or what sector it operates in. This brings the main question which this report will try to answer, namely:

"What makes a port vulnerable to cyber risks?"

Answering this question will help in filling up the current research gap surrounding cyber security in ports. An issue which is found due to the fact that much of academic literature puts their focus on a theoretical approach to cyber security, looking at how supply chain companies could possibly defend themselves against future attacks. This, without looking at what currently seems to attract cybercriminals to a certain target. Creating a clearer picture of what is the cause to current cybercrimes can help in combatting current risks when ports develop and adapt to new circumstances.

I. Does connectivity affect cyber vulnerability in ports?

Introduction

When defining cyber vulnerability by looking at economic size, it becomes interesting to what for an effect a ports connectedness has on its cyber vulnerability. This chapter will first look at if there is a relationship between connectedness and cyber vulnerability on a theoretical basis, after which an OLS regression will showcase the relationship found in the used dataset. Ultimately combining both theory and results to obtain conclusions.

Does more connected mean more vulnerable?

As already highlighted in the literature analysis, Saini et al. (2012) state that for corporations past a certain size and thus international importance, the assessment of economic impacts and consequences of a cybercrime may become a more important factor. But because of the negative implications that come with cybercrime assessment, like the negative publicity it brings and how the value of negative implications of cybercrime are hard to asses, most big firms decide not to report financial historical data regarding cyber-attacks (Saini et al.). This makes assessing the scope of cybercrime in regards to the company very tricky and without help of external bureaus these bigger companies seem to have a hard time deciding as to how much they should spend on cyber vulnerability initiatives (Saini et al.).

Saini et al. state that a more straightforward way to determine as to how much a firm should invest into cyber vulnerability would be an analysis of how big the financial losses would be if the company would be breached, as they call it a “market value approach”. As supply chain companies like ports have seen an increase in value over the last few years, this economic value and importance is only growing (Rivero, 2022). Therefore, it would seem that a port company which has a bigger economic reach and importance and thus sees bigger losses when the infrastructure is shut down by a cyber-attack, would invest more into cyber vulnerability. If they follow this “market value approach”, at least.

Tam & Jones (2018) build upon this thought by underlining that a broader reach facilitated by more connections and a greater network increases the range of cyber-attacks. The further a port’s reach goes, the harder it is to track the target, take into account all laws concerning the network and the harder it becomes to assess every risk (Tam & Jones).

Results from Data

Compiling data retrieved from the yearbooks of Lloyd's List 100 ports together with a dataset posted by the UNCTAD (2020) measuring the top connected ports in early 2020 brings up 44 ports who have both a value attributed to economic size and connectedness. Running an OLS regression on the relationship between the connectedness and the TEU throughputs as listed in Lloyd's list for 2019 shows figures listed in Table 1 below. The results in the first model show a positive significant relationship between the dependent variable representing economic size and connectivity. Showcasing a growth in 0.142 million TEU for every extra direct port connection a port has, ceteris paribus. The model shows a corresponding R^2 value of 0.6111.

Table 1: OLS Regression showcasing relationship between dependent variable 2019 annual TEU throughput (in millions) and independent variable connectivity

	Model
Variable	**(1)**
Connectivity	0.142***
	(0.000)
Constant	-11.978***
	(0.002)
Observations	44
R^2	0.6111

Table Notes: The table describes the relationship between the dependent variable 2019 annual TEU throughput and the independent variable connectivity. Connectivity is measured in absolute numbers. Throughput is measured in millions of TEU. Circular brackets illustrate the variable's p-value. The sample size consists of 44 of the 100 ports listed in Lloyd's List *One Hundred Ports 2021*. ***p< 0.01 ** p<0.05 *p<0.1

Conclusion

When comparing the results shown from the regressions to the theory laid out by Saini et al. (2012) and Tam & Jones (2018), result seems to be in line with theory. Both see similarities with the fact that an increase international reach and connectivity, are paired with an increase in cyber vulnerability spending. The amount at which cyber vulnerability, as stated before, is at a rate of 0.142 million TEU for an increase in direct port connections of 1. This shows a positive significant relationship between connectivity on an international scale and cyber vulnerability.

II. Does main goods type affect cyber vulnerability in ports?

Introduction

Another characteristic of the port that may influence cyber vulnerability is the port's main exporting good. This chapter will weigh off whether a port like Rotterdam who has a lot of liquid bulk throughput sees more cyber vulnerability than a container port, for example the Singapore port. The layout, much like the previous chapter, will consist of a theoretical basis as found in the literature review, results from an OLS regression using the dataset, and ultimately conclusions drawn from both.

Does goods type matter?

Using the OTCAD Stash Kempinski (2021) views the main goal of cyber criminals as that of disrupting the infrastructure of ports and other supply chain nodes targeted in cyber-attacks, rather than that of targeting the victim to directly steal goods and information for monetary value. As Nicolas Rivero (2022) reports, the goal of these criminals seems to be to disrupt the services supply chains provide in such a way that they are pressured to pay even really extreme amounts of money, as every day they are disrupted and thus cannot operate, they are losing money. This begs the question whether the type of supply chain company matters in who these criminals attack or not, as it seems the criminals target the companies based on the high profit margins they make and the large profit numbers they lose when they are restricted from operating (Rivero, 2022).

Basing investments in cyber vulnerability on the fact that criminals will more likely target you if you carry heavier losses when you are shut down seems to point toward the "market value approach" stated by Saini et al. (2012), as highlighted in the previous chapter. This would mean that the type of company and thus also which type of good a port seems to transport the most, play a lesser role in the cyber vulnerability of a pot.

Results from Data

Making use of statistics published in the annual reports and using Lloyd's list information regarding the one hundred ports with the post throughput in 2019, the ports in the dataset can be categorized into categories corresponding to the main goods type in the port. As stated in the chapter on *Methodology & Data*, the categories these ports are divided into are: container, liquid bulk, dry bulk and other; in line with the categories as listed by UNCTAD (2021). This is done by listing the goods type which saw the highest tonnage on an annual basis in 2019, or the main goods type that the port was listed as within either Marine Traffic (n.d.), UNCTAD (2021) or Lloyds' List (2021).

The categorization split the ports up into groups as listed in Table 2 below.

Table 2: Number of ports per goods type category

Category	Number of ports
Container	58
Liquid Bulk	20
Dry Bulk	18
Other	4
Total	100

Table notes: Number of ports per goods type category. Divided into groups by attributing ports to the goods type which saw the highest tonnage in 2019. Tonnages retrieved from annual and trade reports published by the ports, Marine Traffic (n.d.), UNCTAD (2021) or Lloyds' List (2021).

To obtain information regarding the effect this goods type has on cyber vulnerability, as measured in economic size, an OLS regression is run with cyber vulnerability used as the dependent variable, measured in the TEU throughput a port had in 2019. Dummies are used to resemble the categories as shown in the table above. The goods dummy of container ports is used as reference category. As can be seen in Table 3 below, both liquid bulk and dry bulk ports show insignificant negative effects compared to the reference category. The "Other" goods type category shows a significant negative effect, but only represents 4 of the 100 ports in the sample. The R^2 value is listed at only 0.0117. The results point toward the absence of a clear relationship between the cyber vulnerability a port has and the main goods type the port is categorised in.

Table 3: OLS Regression showcasing relationship between dependent 2019 annual TEU throughput (in millions) and independent variables main port goods type.

	Model
Variable	**(1)**
Liquid Bulk	-1.149
	(0.503)
Dry Bulk	-1.189
	(0.623)
Other	-3.278***
	(0.002)
Constant	6.941***
	(0.000)
Observations	100
R^2	0.0117

Table Notes: The table describes the relationship between cyber vulnerability, measured in 2019 annual TEU throughput for a port and main goods type based on throughput on an annual basis. Throughput is measured in millions of TEU. Dummies for main goods type are categorized by looking at highest throughput for goods type in 2019. Circular brackets illustrate the variable's p-value. The sample size consists of the 100 ports listed in Lloyd's List *One Hundred Ports 2021*. ***p< 0.01 ** p<0.05 *p<0.1

Conclusion

Much like the literature and articles by Kempinski (2021) and Nicolas Rivero (2022) state, it seems that the type of company being targeted does not matter besides it being a logistical or supply chain company. The main importance for the cyber-attackers is solely that of being able to gain as large of a ransom amount as possible, as Nicolas Rivero states. The amount they can ask as a ransom seems to be greater when the company has bigger losses when it is shut down, in line with Saini et al.'s (2012) market value approach. The results from the regression reflect this idea. Seeing little to no significant differences between the goods types, pointing towards the idea that the vulnerability for cyber-attacks is caused by other factors.

III. Does geographic region affect cyber vulnerability in ports?

Introduction

The last port characteristic that will be investigated, is that of geographic region. Much of the reasoning behind this is to test whether cyber criminality is a factor which shows more prominence in certain world regions as compared to others. This will first be analysed using the literature review, afterwards the dataset will be analysed using an OLS regression examining if some regions see disproportionately more spending than others.

Cyber criminals in different world regions

The factor of geographic region brings with it many regional elements which could affect cyber vulnerability. These can be based on a regions culture, population or many other aspects tied to a certain region. Research of which countries are most targeted, like that of Bendovschi (2015), show that North America and Europe come out on top. With the likes of the USA, Russia, Germany and the Netherlands being the main victims of these cybercrimes.

Fontanilla (2020) lists much of the same countries having cyber issues, with high cyber vulnerability issues in recent years fuelled by an increase in cyber messaging due to the COVID pandemic. Besides the countries already listed by Bendovschi however, Fontanilla also mentions Japan and Taiwan as high-profile victims of cyber-attacks, shedding more light on the Asian continent as a targeted group.

Other articles, like that of Ghosh & Turrini (2010) looks differently at this, stating that cybercrime is less so an issue for specific countries, but more an issue which transcends national borders and impacts all countries worldwide equally. Ghosh & Turrini point towards the internet of things being an uncontrolled landscape which, with the absence of one clear governing body, seems to make nations and jurisdiction for cybercrimes a very complicated matter. They state that the scope of cybercrimes will only extend into every country and are of the world where technological systems are used to achieve goals, making it so all countries must invest into cyber protection.

Results from data

Data from 100 ports listed in the Lloyds's list will be taken into account when running a regression on the relationship per world region. The model which takes into account the world regions together with the connectivity variable uses data from the 44 ports who were listed in the UNCTAD 2020 list. Model 1 below looks at the relationship between cyber vulnerability, measured in economic size, and world continental regions, as listed by Lloyds' list (2021). The second model showcases the same dependent variable, cyber vulnerability, but this time compares it to the world trade regions listed in Lloyds' list.

This to test whether these region effects differ from those on a continental definition of geography. Finally, the significant variable connectivity from Table 1 is implemented into the same set of independent variables as Model 1 to see its effects when combined with the geographic regions.

Table 4: OLS Regression showcasing relationship between dependent variable 2019 annual TEU throughput (in millions) and independent variables port continental region and port trade region.

	Model		
Variable	**(1)**	**(2)**	**(3)**
Asia	3.638**		9.479***
	(0.015)		(0.000)
North America	0.308		2.971*
	(0.977)		(0.098)
Africa	-1.622*		4.419**
	(0.099)		(0.021)
South America	-1.413		4.496*
	(0.112)		(0.074)
Oceania	-1.844**		-
	(0.027)		-
Mediterranean		-5.022***	
		(0.001)	
Middle East		-4.219**	
		(0.035)	
Northern Europe		-2.917	
		(0.148)	
North America		-4.002**	

Table 4 (continued)

		(0.012)	
Oceania (region)		-5.877***	
		(0.000)	
Central & South America		-5.446***	
		(0.000)	
Africa (Region)		-6.426***	
		(0.000)	
Connectivity			0.136***
			(0.000)
Constant	4.528***	8.561***	-16.670***
	(0.000)	(0.000)	(0.000)
Observations	100	100	44
R^2	0.0827	0.1005	0.7980

Table Notes: The table describes the relationship between cyber vulnerability, measured in 2019 annual TEU throughput and the continental region a port is located in, illustrated as a set of dummies in column 1. And the relationship between cyber vulnerability and the world trade region a port is located in, illustrated as a set of dummies in column 2. Column 3 showcases the dummies listed in model 1 with the addition of the variable connectivity, as tested significant in the previous chapter. Throughput is measured in millions of TEU. Circular brackets illustrate the variable's p-value. The sample size consists of the 100 ports listed in Lloyd's List *One Hundred Ports 2021*. ***p< 0.01 ** p<0.05 *p<0.1

Making use of a dummy variable stating the effect location measured in world continent, the relationship is shown, illustrated in Table 4. This OLS regression makes use of the "Europe" dummy as reference category. As the table illustrates in Model 1, the Asian port region seems to have higher expenditures relative to Europe, showing a significant positive value over the reference category. North America shows non-significant positive effects in expenditure over Europe. Both Africa and Oceania show negative differences compared to the European region. Both these regions show significant effects.

South America shows slightly unsignificant negative effects. Using the continental regions as dummies in the model showcases an R^2 of 0.0827.

If we then run the same regression making use of Lloyd's List's categories defining port regions, we can view the results from a different point of view. Making use of the Far East region (Asia excluding Middle East) as reference category, Model 2 showcases the difference the other regions have as compared to the Far East Asia region. The model shows that all other regions have negative effects as compared to the reference category. With Northern Europe not having significant negative effects, the North America and Middle East region having slightly significant negative effects and the Mediterranean, Africa, Central & South America and Oceania regions having significant negative effects. Defining the dummies by making use of the trade regions as stated in Lloyd's list (2021) showcases an R^2 of 0.1005.

Both models show that the Asia continental region, and especially when defined as the Far East Asia trade region (as seen by Model 2), has the highest cyber vulnerability. Something which can be seen back in the fact that 7 of the 10 highest spenders on cyber expenses are located in the Far East Asian trade region.

When accounting for throughput as a variable as is done in Model 3 of Table 4, the significance of the North American, South American an African continents shifts from being non-significant to significant and the Asia continental region remains significant and very positive. Much like in the first sub-question, connectivity shows very significant positive effects, at a bit lower level compared to that of Table 1. The model showcases an R^2 of 0.7980.

Conclusion

The results from data show significant high positive effects when a port is located in the Asian region compared to the European region. And slightly significant negative effects when it is located in Oceania or Africa compared to Europe. Looking at the Far East trade region as reference category shows that the Far East Asian ports have significantly higher cyber vulnerability compared to the other trade regions, excluding Northern Europe which sees non-significant negative effects. When taking into account the connectivity variable as part of the model all continental region seem to remain or change to a significant positive effect as compared to Europe. Something which points to a big part of the effect being attributed to the connectivity. Both with and without taking account connectivity these model results support some claims made in the beforementioned literature and contradict others. The results tend to resemble the top countries listed by Fontanilla (2020) more than those claimed by Bendovschi (2015), including top Asian countries as high victims of cybercrime.

Both list Europe and North American countries, which in the results from data both also show higher numbers than the remaining world regions, except when connectivity is taken into account. All in all, however, it does seem to make an impact in which world region it is located for the cyber vulnerability of a port, not yet resembling a world where location does not matter in terms of cybercrime and all countries spend in a balanced way, like Ghosh & Turrini (2010) state.

Summary of Results

Introduction

This chapter will focus on the summarization of the previous three sub-questions. It will quickly sum up the main findings in those chapters, found both in theory and the regressions. This will give a general picture of some interesting trends that can be drawn from the found results. In that way building up to the following chapter which will draw conclusions from these results.

Results

When testing for the effect of characteristics of the port on cyber spending, the previous chapters looked at connectivity, main goods type and location where the port is located. By using regressions to view the effect these characteristics have on cyber vulnerability, which is illustrated by economic size, it allows for the illustration of a so-called port profile which would see the most vulnerability, and in that way feel as though it is more susceptible to cyber-attacks and risks.

The first characteristic, connectivity, was one which was shown as having a significant effect on cyber vulnerability. Seeing an increase in cyber vulnerability as the amount of direct port connections grew. This was in line with literature, showing that a port with a greater reach and network seems to have bigger losses when it is attacked, because its network impact is affected more. After concluding this, the next step was to test whether the different goods types seen in ports around the world would make a difference for the level of expenditures, having the ports divided into categories following goods types as listed by the UNCTAD (2021). Literature showcased a trend in cybercrime that criminals did not choose their targets based on the company product type or sector but focused more on the losses the company would have in case of an infrastructure disruption, allowing them to demand high ransom fees. This was backed by the results from the dataset, which saw insignificant results between the categories, meaning that there was a low probability that goods type had an effect on the cyber vulnerability of a port. The final characteristic that was tested was the location in the world the port was located in. Literature on cyber-crime saw that certain countries were more frequently a cybercrime victim than others. Results from data showed either a significantly higher level of vulnerability in Asia or North America when compared to Europe, depending on the model used to measure this effect. Both these results were in line with literature, which listed the USA and Asian countries as high targets on the list of cybercrime victims. Pointing towards where a port was located on a world scale making a difference as to how cyber vulnerable they are.

Compiling all characteristics to create a general model brings the results found in Appendix A.3., where it shows a significant positive effect for connectivity and a significant negative effect for all regions compared to the Asian region, except South America, which is not significant.

Much like in the separate models, product type does not show very significant effects, only highlighting either positive or negative differences from the reference category container port, besides "Other" goods type, which sees significant positive effects. The R^2 is showcased at a level of 0.8167.

Assumptions & Constraints

Making use of the economic size of a port to see to what extent characteristics of a port affect the cyber vulnerability doesn't fully paint a relationship between cyber vulnerability itself and the characteristics, but more so creates a proxy which can be linked to ports being more cyber vulnerable if they are bigger in economic size. Because of this, this research does not fully reflect the direct effect these risks have on the ports, because there could be factors which are overlooked but still have underlying effects on the results seen in the OLS regressions. Linking the amount of cyber-attacks or threats to the different ports would better showcase this relationship, but due to the current unavailability of data regarding these numbers, mostly because ports are not obliged to share this information, makes it so researching this relationship becomes difficult.

Also, the size of the sample is quite limited due to only 44 of the 100 ports having their connectivity numbers mentioned by the UNCTAD. This sample size only reflects the top 100 ports of the time period, leaving out ports which are not placed on this list and have lower levels of TEU throughput and international reach. Because many of the ports on the list are located in Asia, there is an overrepresentation of this continent, with Oceania Africa and South America seeing low representation.

Conclusions & Discussions

Introduction

This final chapter will use the results found in the three sub-questions and summarized in the previous chapter, together with literature, to answer the paper's main question. After this conclusion a list of suggestions and statements will be made in the discussion segment on how the research could be further broadened.

Conclusions

As a way to try to answer the main question, this paper made use of literature regarding cybercrime and technology in the maritime world and the world as a whole, together with models testing the effects of specific characteristics of ports. Using these results to create a profile of the most vulnerable target in cyber terms allows for the interpretation of what seems to pull cyber criminals to certain ports over other, in that way determining:

"What makes a port vulnerable to cyber risks?"

When looking at the results from the sub-questions, it seems that connectivity, defined by the amount of direct port connections a certain port has, is a main factor connected to cyber vulnerability. It shows significant positive effects in all models tested in this paper. Even when other variables calculating location and goods type are added connectivity is something which keeps showing up as a significant factor related to the cyber vulnerability of a port. Ports seem to follow the "market value approach" laid out by Saini et al. (2012), which states that a firm determines the value attributed to investments in cyber vulnerability by looking at the impact it would have would the company be disrupted, determined by the capital value of the company. A higher profile port seems to be more vulnerable to cyber risks than one which has a lower network reach. Where a port is located also seems to make an impact on its vulnerability for cyber risks. Both Fontanilla (2020) and Bendovschi (2015) list that certain countries are more often targeted by cybercrimes than others. They state that countries like the USA, Taiwan, Japan and Germany are more vulnerable to cyber-attacks than others based on the number of attacks they are a victim of. The models seem to reflect this statement, seeing Asian ports be more vulnerable when looking at absolute values, and when accounting for economic size as an additional variable. Main goods type, however, categorized by looking at what goods type sees the most tonnage on an annual basis in a port, does not seem to make a difference for the vulnerability of a port.

The model shows insignificant effects when looking at differences between the cargo types, meaning a focussing on a different good does not alter how vulnerable you are for cyber risks. This is also found in literature like that of Kempinski (2021), which states that cyber criminals do not look at the company type they are attacking to determine their targets, but seem to focus more on the impact their disruptions will have on the company.

To summarize and answer the question listed above, based on the research found in this paper, it seems as though a port's cyber vulnerability, as determined by its economic size, becomes more vulnerable when a port has more direct port connections. It becomes especially more vulnerable when it is located in Asia, and does not become more vulnerable when it mainly throughputs a certain goods type, compared to another. Factors which are positively correlated with the economic size of the port in turn reflect a greater vulnerability.

Discussions

As stated in the previous chapter, this report is constrained in both sample size and data availability. Further research could make use of other variables to test whether economic size is a good reflection of cyber vulnerability as a whole and within the port landscape. Other possibilities would be to extend the sample to correspond equal quantities of all port regions, types and look at throughput numbers lower than those listed on Lloyd's list.

Cyber security and vulnerability within the maritime world are two things which have only really come to the forefront during recent years, as cyber dependence has increased within all facets of the industry. Looking into ways ports can combat this issue and become more aware of the dangers it proposes is essential for the future protection of the industry. As technological dangers will become more frequent, it's important that these important supply chain nodes find ways to keep invaders out and avoid having major shutdowns with international effects.

Appendix

Appendix A.1.: List of all ports registered in Lloyd's List One Hundred Ports (2021)

Ranking	Port	Country	Continent	Ranking	Port	Country	Continent
1	Shanghai	China	Asia	51	Felixstowe	United Kingdom	Europe
2	Singapore	Singapore	Asia	52	Dongguan	China	Asia
3	Ningbo-Zhoushan	China	Asia	53	Seattle/Tacoma	United States	North America
4	Shenzhen	China	Asia	54	Yantai	China	Asia
5	Guangzhou	China	Asia	55	Incheon	South Korea	Asia
6	Qingdao	China	Asia	56	Abu Dhabi	United Arab Emirates	Asia
7	Busan	South Korea	Asia	57	Gioia Tauro	Italy	Europe
8	Tianjin	China	Asia	58	Balboa	Panama	South America
9	Hong Kong	China	Asia	59	Cartagena	Colombia	South America
10	Rotterdam	The Netherlands	Europe	60	Tangshan	China	Asia
11	Dubai	United Arab Emirates	Asia	61	Nanjing	China	Asia
12	Port Klang	Malaysia	Asia	62	Houston	United States	North America
13	Antwerp	Belgium	Europe	63	Melbourne	Australia	Oceania
14	Xiamen	China	Asia	64	Barcelona	Spain	Europe
15	Tanjung Pelepas	Malaysia	Asia	65	Manzanillo	Mexico	North America
16	Kaohsiung	Taiwan	Asia	66	Ambarli	Turkey	Europe
17	Los Angeles	United States	North America	67	Chittagong	Bangladesh	Asia
18	Hamburg	Germany	Europe	68	Virginia	United States	North America
19	Long Beach	United States	North America	69	London	United Kingdom	Europe
20	Ho Chi Minh City	Vietnam	Asia	70	Yokohama	Japan	Asia
21	New York/New Jersey	United States	North America	71	Kobe	Japan	Asia
22	Laem Chabang	Thailand	Asia	72	Durban	South Africa	Africa
23	Tanjung Priok	Indonesia	Asia	73	Genoa	Italy	Europe
24	Colombo	Sri Lanka	Asia	74	Nagoya	Japan	Asia
25	Tanger Med	Morocco	Africa	75	Oakland	United States	North America
26	Mundra	India	Asia	76	Marsaxlokk	Malta	Europe
27	Yingkou	China	Asia	77	Le Havre	France	Europe
28	Piraeus	Greece	Europe	78	Sydney	Australia	Oceania
29	Valencia	Spain	Europe	79	Osaka	Japan	Asia
30	Taicang	China	Asia	80	Charleston	United States	North America
31	Hai Phong	Vietnam	Asia	81	Quanzhou	China	Asia
32	Dalian	China	Asia	82	Callao	Peru	South America
33	Algeciras	Spain	Europe	83	Yeosu Gwangyang	South Korea	Asia
34	Rizhao	China	Asia	84	King Abdullah	Saudi Arabia	Asia
35	Lianyungang	China	Asia	85	St Petersburg	Russia	Europe
36	Bremen/Bremerhaven	Germany	Europe	86	Karachi	Pakistan	Asia
37	Jeddah	Saudi Arabia	Asia	87	Guayaquil	Ecuador	South America
38	Savannah	United States	North America	88	Haikou	China	Asia

Ranking	Port	Country	Continent	Ranking	Port	Country	Continent
39	Jawaharlal Nehru	India	Asia	89	Jiaxing	China	Asia
40	Colón	Panama	South America	90	Mersin	Turkey	Europe
41	Manila	Philippines	Asia	91	Gdansk	Poland	Europe
42	Cai Mep	Vietnam	Asia	92	Nantong	China	Asia
43	Salalah	Oman	Asia	93	Dammam	Saudi Arabia	Asia
44	Tokyo	Japan	Asia	94	Zhuhai	China	Asia
45	Santos	Brazil	South America	95	Taichung	Taiwan	Asia
46	Port Said	Egypt	Asia	96	Southampton	United Kingdom	Europe
47	Qinzhou	China	Asia	97	Izmit	Turkey	Europe
48	Tanjung Perak	Indonesia	Asia	98	Lomé	Togo	Africa
49	Fuzhou	China	Asia	99	Alexandria	Egypt	Africa
50	Vancouver	Canada	North America	100	Jinzhou	China	Asia

Table Notes: Top 100 ports of 2021 based on TEU throughput numbers of 2020. Source: Lloyd's List (2021)

Appendix A.2.: Variable names and explanation

Variable name	Explanation	Measured in
Ranking	Ranking from 1 to 100 on Lloyd's List of 2021's hundred highest ranked ports, based on TEU throughput the ports had in both 2019 and 2020.	Values between 1 and 100
Asia	Dummy variable which indicates whether a port is located in the continent of Asia, for which it then contains the value 1. If the port location is anything other than Asia this dummy variable has a value of 0.	Either value of 1 or 0
Africa	Dummy variable which indicates whether a port is located in the continent of Africa, for which it then contains the value 1. If the port location is anything other than Africa this dummy variable has a value of 0.	Either a value of 1 or 0
North America	Dummy variable which indicates whether a port is located in the continent of North America, for which it then contains the value 1. If the port location is anything other than North America this dummy variable has a value of 0.	Either a value of 1 or 0
Oceania	Dummy variable which indicates whether a port is located in the continent of Oceania, for which it then contains the value 1. If the port location is anything other than Oceania this dummy variable has a value of 0.	Either a value of 1 or 0
Europe	Dummy variable which indicates whether a port is located in the continent of Europe, for which it then contains the value 1. If the port location is anything other than Europe this dummy variable has a value of 0.	Either a value of 1 or 0
2019 annual throughput (TEU)	Continuous variable which illustrates amount of TEU unit's throughput a port had in the year 2019.	Measured in millions of TEU ranging from 1.500611 to 43.303000 TEU.
Cyber expenditures	Continuous variable which illustrates amount spent on cyber vulnerability and awareness in the year 2019 by a port.	Absolute value of expenditures in either IT or Software as retrieved from the port's annual report,

		measured in US Dollars. When values were stated in a foreign currency these have been exchanged with exchange rates measured on the 31st of December 2019.
Container	Dummy variable which indicates whether a port has container goods as highest throughput of a goods type. If the main goods type is containers, the dummy value is 1, otherwise it is 0.	Either a value of 1 or 0
Liquid Bulk	Dummy variable which indicates whether a port has liquid bulk goods as highest throughput of a goods type. If the main goods type is liquid bulk, the dummy value is 1, otherwise it is 0.	Either a value of 1 or 0
Dry Bulk	Dummy variable which indicates whether a port has dry bulk goods as highest throughput of a goods type. If the main goods type is dry bulk, the dummy value is 1, otherwise it is 0.	Either a value of 1 or 0
Other	Dummy variable which has a value of 1 if the port does not have containers, liquid bulk or dry bulk as main goods type. If one of the beforementioned goods type is the ports main goods type, this variable has a value of 0.	Either a value of 1 or 0
Connectivity	Numerical variable which represents the direct port connections a port has. If this variable is high a port is well connected on an international scale. If this variable is high a port often transhipps via other ports.	Measured in absolute numbers ranging from 92 (Balboa) to 288 (Shanghai).

Appendix A.3.: OLS regression showcasing relationship between dependent variable 2019 annual TEU throughput (in millions) and all independent variables tested for in this paper.

	Model
Variable	**(1)**
Connectivity	0.139***
	(0.000)
Europe	-9.911***
	(0.000)
North America	-6.625***
	(0.000)
Africa	-7.299***
	(0.000)
South America	-2.085
	(0.439)
Liquid Bulk	-3.452
	(0.238)
Dry Bulk	0.505
	(0.883)
Other	3.312***
	(0.000)
Constant	-6.974**
	(0.040)
Observations	44
R^2	0.8167

Table Notes: The table describes the relationship between economic size for a port and the continental region a port is located in, a ports connectivity and the main goods type it throughput in 2019. Main goods type and continental location are illustrated as a set of dummies, TEU throughput is illustrated as a continuous variable. Throughput is measured in millions of TEU. Connectivity is measured in absolute values. Circular brackets illustrate the variable's p-value. The sample size consists of 44 of the 100 ports listed in Lloyd's List *One Hundred Ports 2021*. ***p< 0.01 ** p<0.05 *p<0.1

References

- Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*, *2*(1), 123-138.
- Balcombe, P., Brierley, J., Lewis, C., Skatvedt, L., Speirs, J., Hawkes, A., & Staffell, I. (2019). How to decarbonise international shipping: Options for fuels, technologies and policies. *Energy conversion and management*, *182*, 72-88.
- Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24-31.
- CSIS (2022) *Significant Cyber Incidents Since 2006.* Retrieved on the 22nd of April via: https://csis-website-prod.s3.amazonaws.com/s3fs-public/220404_Significant_Cyber_Incidents.pdf?6baqc92oMg0w.0wCwZLP6OATs9MmMmLG
- DNV (n.d.) Digitalization in the Maritime industry. Retrieved on the 1st of May via: https://www.dnv.com/maritime/insights/topics/digitalization-in-the-maritime-industry/index.html
- Donepudi, P. K. (2014). Technology growth in shipping industry: an overview. *American Journal of Trade and Policy*, *1*(3), 137-142
- Ducaru, S. (2016). Is Cyber Defense Possible? *Journal of International Affairs*, *70*(1), 182–189. https://www.jstor.org/stable/90012603
- FERM (2016) *Wat is FERM.* Retrieved on the 17th of June via: https://www.ferm-rotterdam.nl/nl/column/column-rene-de-vries
- Fontanilla, M. V. (2020). Cybercrime pandemic. *Eubios Journal of Asian and International Bioethics*, *30*(4), 161-165.
- Ghosh, S., & Turrini, E. (Eds.). (2010). *Cybercrimes: A multidisciplinary analysis*. Springer Science & Business Media.
- Harvard Business Review (2018) *Software Asset Management: A New Defense Against Cybersecurity Threats.* Retrieved on the 21st of May via: https://hbr.org/sponsored/2018/03/software-asset-management-a-new-defense-against-cybersecurity-threats
- Kempinski, S. (2021) OTCAD. OPERATIONAL TECHNOLOGY CYBER ATTACK DATABASE. Retrieved on the 22nd of April via: https://securitydelta.nl/media/com_hsd/report/442/document/Secura-White-Paper-OTCAD.pdf

- Le Journal de la Marine Marchande (2020) *Rapport: Les cyberattaques maritimes ont augmenté de 400 %.* Retrieved on the 1st of May via: https://www.journalmarinemarchande.eu/filinfo/rapport-les- cyberattaques-maritimes-ont-augmente-de-400
- Lloyd's List (2021) *One Hundred Ports 2021.* Retrieved on the 23rd of April via: https://lloydslist.maritimeintelligence.informa.com/-/media/lloyds-list/images/top-100-ports-2021/top-100-ports-2021-digital-edition.pdf
- Maersk (2017) *2017 September Maersk Post Full Issue*. Retrieved on the 17th of June via: https://www.maersk.com/~/media_sc9/maersk/corporate/press/publications/files/2017-september-maersk-post-full-issue.pdf
- Maersk (2020) *The 2017 Maersk Cyber Incident.* Retrieved on the 17th of June via: https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf
- Marine Traffic (n.d.) *Port Call Statistics. Port of Nanjing.* Retrieved on the 21st of April via: https://www.marinetraffic.com/en/ais/details/ports/2745?name=NANJING&country=China#Statistics
- McKinsey & Company (2019) *Perspectives on transforming cybersecurity.* Retrieved on the 20th of May via: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx
- Millefiori, L. M., Braca, P., Zissis, D., Spiliopoulos, G., Marano, S., Willett, P. K., & Carniel, S. (2021). COVID-19 impact on global maritime mobility. *Scientific reports*, *11*(1), 1-16.
- OANDA (n.d.) Currency Converter. Retrieved on the 9th of May via: https://www.oanda.com/currency-converter/en/?from=CNY&to=EUR&amount=1
- PSA International (2020) *Unfolding the Future, Annual Report 2019*. Retrieved on the 1st of May via: https://www.globalpsa.com/wp-content/uploads/AR2019.pdf
- Qinhuangdao Port Co. (2020) *Annual Report 2019.* Retrieved on the 1st of May via: https://media-portqhd.todayir.com/20200422005931179816546 6_en.pdf
- Rivero, N. (2022) *Ransomware hackers are now going after supply chain companies.* Quartz. Retrieved on the 9th of May via: https://qz.com/2132444/ransomware-hackers-are-now-going-after-supply-chain-companies/
- Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

- Stormshield (2021) *Cybermarétique: a short history of cyberattacks against ports.* Retrieved on the 21st of April via: https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/
- Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147-164.
- UNCTAD (2020) *Ports in the global liner shipping network: Understanding their position, connectivity, and changes over time.* Retrieved on the 20th of June via: https://unctad.org/news/ports-global-liner-shipping-network-understanding-their-position-connectivity-and-changes-over
- UNCTAD (2021) *Review of Maritime Transport 2021.* Retrieved on the 19th of April via: https://unctad.org/system/files/official-document/rmt2021_en_0.pdf