Assessment of systemic vulnerabilities in container shipping networks with consideration of transhipment

Pablo E. Achurra-Gonzalez[1], *Panagiotis Angeloudis,*
Nils Goldbeck, Konstantinos Zavitsas, Daniel J. Graham, Marc Stettler

Centre for Transport Studies
Department of Civil & Environmental Engineering
Imperial College London

Abstract

The global container shipping network is vital to international trade. Current techniques for its vulnerability assessment are constrained due to the lack of historical disruption data and computational limitations due to typical network sizes. We address these modelling challenges by developing a new framework, composed by game-theoretic attacker-defender model and a cost-based container assignment model that can identify systemic vulnerabilities in the network. Our analysis illustrates the differences in vulnerability and port criticality rankings with different disruption magnitudes. Model outputs are used to establish performance baselines and to assess the effectiveness of component-level interventions seeking to increase network resilience.

1 Introduction

Ocean shipping is the principal mode of international freight transport, underpinning global trade [1]. Frictionless and stable access to the container shipping services has been shown to be a pivotal contributor to trade competitiveness of any national economy. Otherwise referred to as liner shipping services, these can be described as scheduled, recurring sequences of port calls, operated by ocean carriers and shipping alliances. Collectively, they form the global liner shipping network, with ports represented as nodes, and links being defined as the vessel journeys between successive port calls within each service.

An important aspect to consider when assessing liner shipping vulnerabilities is the presence and proportion of transhipment operations in the network. Transhipment is of critical importance for trade lanes with large cargo volumes (e.g. Asia-to-Europe), where ocean carriers deploy larger vessels on inter-regional legs to benefit from economies of scale. In hub-and-spoke systems of this nature, transhipment ports facilitate container flows that could not have been served with direct services. As such, liner service networks with a high dependence on a small cluster of transhipment hubs are expected to be particularly vulnerable to disruptions. Furthermore, and as illustrated by recent events, any potential disruptions to this network can have significant and immediate implications for consumers, industries, markets, and national economies. Potential sources of disruption include natural disasters (earthquakes, floods), political conflicts (wars, blockades, piracy), and market events (bankruptcy of ocean carriers, fuel price fluctuations).

The nature, location, and severity of these disruptions may pose significant threats to the ability of the network to accommodate cargo flows. It is therefore crucially important to understand how such disruptions would affect public and private stakeholders that are responsible for ensuring its operability and accessibility [2]. This can be achieved through the application of quantitative frameworks that identify the critical network components [3] and evaluate the effectiveness of preventive interventions [4].

The complex structure of the liner shipping industry and the inherent relationships among market participants do not readily lend themselves to mathematical analysis and formulation. Previous studies on liner shipping vulnerability relied mostly on complex network models, which can be classified as either pure-topological or flow-based models [5], [6]. The majority of pure-topological models (sometimes also referred to as zero-degree models [7]) focus on indicators such as degree distributions and the betweenness centrality of network components [8] to evaluate network vulnerabilities, without directly considering material flows or commercial activity. In contrast, flow-based models (e.g. one- or n-degree models) use costs, operational and

[1] Corresponding author. p.achurra-gonzalez@imperial.ac.uk

physical constraints to describe the overall performance of the networks, and model the redistribution of vessel movements or material flows in the aftermath of disruptions [9].

Although pure-topological models provide a straightforward approach to critical component rankings [10]–[12], they mainly adopt binary network representations (e.g. presence of a connection between two ports). Such representations cannot be readily used to evaluate the impact of disruptions on network capacity, travel times or processing times [3], nor to quantify any costs of cargo rerouting or potential gains from disruption prevention. Furthermore, they are only applicable to scenarios involving a complete loss of network components. However, such approaches do not transfer well to the study of transport networks, where partial component disruptions are frequent, if not the norm. Sullivan et al. [13] argue that the main problem of pure-topological models is the creation of isolated sub-networks that are inaccessible after component removal. These limitations can severely restrict studies on liner shipping operations, where partial disruptions (e.g. March 2013 labour strike that reduced the capacity of the Hong Kong port-system by 20% [14]) are more frequent than complete failures. Furthermore, isolated sub-networks are less likely in liner shipping, as vessels and cargoes can be rerouted.

In contrast, flow-based models can capture the re-distribution of commodity flows subject to capacity limitations inherent to existing network configurations. Where historical disruption data is available, it is possible to implement probabilistic flow-based approaches to quantify the network vulnerability based on the expectations of failure of network components [7]. However, the variety of actors and processes within modern liner shipping networks, the complexity of their relationships, and industry confidentiality practices make it problematic and uneconomic to collect and maintain historical disruption data on network components. Therefore, the application of these approaches is mostly compromised by their dependence on sets of data which are often confidential or not available in the liner shipping industry [15].

Previous studies evaluated the applicability of flow-based models for the vulnerability assessment of liner shipping network disruptions and their effects on the ability of the network to meet container transport demand. Even though some considered industry practices such as empty container repositioning [16], [17], transhipment across shipping alliances, and vessel schedule recovery after disruptions, most of these methodologies are limited in terms of the network size that they can evaluate. This limitation prohibits the analysis of global large-scale realistic network instances that would be of interest to private operators or public entities.

Examples of flow-based models include the frequency and cost-based container assignment models by Bell et al. [18], [19] which used a transit assignment and task network approach [20] to represent liner shipping operations. Both studies assume that sufficient capacity (in links and nodes) exists in the transport network to meet transport demands between ports. Such an assumption would not translate well to disrupted liner shipping networks where a significant portion of the overall liner or port handling capacity in the system has been compromised.

In summary, there exist two inherent modelling challenges in the study of liner shipping resilience: (i) lack of historical disruption data (ii) lack of quantitative models capable of representing liner shipping operations at a global scale. The first inhibits the implementation of methodologies that require prior knowledge of disruption probabilities to quantify the vulnerability of the network. The second creates the need for models capable of capturing key industry practices such as transhipment, empty container repositioning, and the ability of vessels to skip disrupted ports while at the same time allowing for implementations at realistic large-scale liner shipping networks.

The objective of this study is to address these challenges by developing a new systemic vulnerability analysis framework that can identify critical components in large-scale liner shipping networks with little or no historical disruption data. We build upon the Ouyang et al. [5] definition of vulnerability and the Qiao et al. [3] system-level approach to define systemic vulnerability as the performance drop of a transport system (e.g. in terms of routing costs or connectivity) given a disruptive event.

The proposed framework consists of two components, with the first being a game-theoretic attacker-defender model (ADM), between a malevolent agent (attacker) and an ocean carrier or alliance (defender). The second component is a container assignment model (CAM) that predicts container flows given a specific liner service structure, port capacities and market demand. The resulting integrated model (ADCAM) is used to evaluate the merits of either player's strategies, and applied to a large problem instance, with 88 services, 230 ports, 2,648 origin-destination (OD) demand pairs and 242,214 weekly container movements.

In addition to flow rerouting, this approach can measure the impact of disruptions in terms of additional handling costs and non-delivery penalties. The model also considers port call skipping, a common practice by

ocean carriers for dealing with service disruption. Its principal output is a matrix of component attack probabilities, used to identify and rank critical components and calculate financial gains from disruption prevention.

The premise, assumptions and structure of this framework are presented in section 2, which provides the formulations of the constituent mathematical problems. A case study involving disruptions at major European container ports and services is presented in section 3, followed by a discussion on how costs and criticality rankings are affected by disruptions levels and flow diversion strategies. The paper concludes with a summary of contributions, limitations, and suggestions for future work.

2 Methodological framework

This section presents the attacker-defender cost-based assignment model (ADCAM) and its integration with the non-cooperative game-theoretic framework to identify the most critical components in liner shipping networks exposed to disruptions. We also present a linear formulation of the model, that allows for implementations on large liner shipping networks drawn from practice. The scalability of the methodology is tested using numerical case studies developed in later parts of this paper.

2.1 Cost-based container assignment model (CAM)

Container assignment models seek to determine optimal container flows from origin ports $k \in K$ to destination port $s \in S$, across a sequence of attractive liner service leg (a "virtual" link, connecting any pair of ports within a service) that can reduce the overall routing costs in the system. The resulting flows will take place upon a set of optimal flow paths, that in the first instance are expressed as chains of legs belonging to one or more services. Given that vessel arrival and departures at a given port k are assumed to be random and uncoordinated (see assumption 2.4), the availability of attractive legs at k is proportional to the frequencies of services that can connect k to s. Therefore, the dwell times of s-bound containers at k is equal to the inverse sum of their service frequencies [18]. In contrast, direct shipments do not incur dwell times. Due to considerations of port and service capacity, it is possible and acceptable for the model to establish multiple flows for each OD pair, each with a different path.

An earlier study [15] proposed the use of penalties for any cargo demands that cannot be satisfied by the assignment process. Such penalties are particularly useful for problem instances where network capacities (at ports or services) could not satisfy the transport demand in the aftermath of disruptions and are used to quantify disruption impacts, and redundancy levels (residual capacity to re-route transport demands).

Our study uses higher penalty values for full containers, to prioritise cargo deliveries over empty container repositioning (e.g. USD 50,000 per full container as opposed to USD 5,000 for empties). It should be noted that the inclusion of empty container repositioning in this study (introduced and discussed later in this paper) captures the impact of the excessive accumulations of empty containers not repositioned in the network, which can ultimately slow down or halt port operations.

A potential limitation of the approach presented in [15] relates to the emphasis on individual network components, which precluded the study of more complex scenarios that involve disrupted natural corridors (such as canals, straits, access channels). This was partially addressed in [2], which introduced further dimensions to the representation of network elements to capture network component dependencies upon such corridors. A vessel routing algorithm was used to automatically include such dependencies, using a set of predefined geographical limits for major maritime corridors in the network (Figure 2.1). The following assumptions are used to formulate the mathematical model for container assignment used in this study:

Assumption 2.1: Loaded containers are assumed to have a fixed set of daily rent, uniform loads, handling priorities, and cargo depreciation rates.
In practice, ocean carriers may utilise varying rental cost structures for shippers, as a result of bespoke commercial contracts and bilateral shipment agreements. Similarly, shippers will incur specific cargo depreciation costs depending on shipment values and cargo types. Finally, repositioning costs may be included in freight rates in trade lanes with high trade imbalances.

Given that not all trade routes and shippers are affected by such practices (e.g. due to negotiated volume-based shipment contracts), the accurate inclusion of such distinctions would have required access to trade

transaction data, which are often confidential and generally unavailable for academic research. The values used in this study are commensurate to the pricing structures employed in previous studies by Bell et al. [18], [19] as shown in Table 3.1. This assumption simplifies data requirements and assumes that all cargo transported through the network is equally prioritised. Nevertheless, the model formulation is sufficiently flexible and readily adaptable by practitioners who are privy to such information.

Assumption 2.2: An exogenous OD demand matrix is used as model input, with weekly demand rates being fixed across the period surveyed.
Demand for container cargo transport can vary on each OD pair and aggregate trade lanes based on factors such as seasonality, changes in markets structures (e.g. trade tariffs), or disruptive technologies. As this model is intended for use in strategic network design, we deemed this assumption acceptable for this study. Furthermore, a weekly time-window is used for container routing, which we regard as sufficiently small to absorb minor demand variations.

Assumption 2.3: Empty containers incur a penalty cost if not transported.
The inclusion of a penalty cost for empty containers not transported serves two purposes: First, the maximisation of empty containers repositioned in the network when there is available capacity (either in the baseline case or after disruptions). If empty container penalties are omitted, the model can provide feasible solutions where no empty container is repositioned (even if capacity is available in the aftermath of disruptions) due to the cost minimisation approach in the objective function.

Note that loaded container penalties in our model are always higher than for empty containers (e.g. USD 50,000 for loaded and USD 5,000 for empties, as discussed in section 3). Therefore, the routing of full containers will be prioritised over repositioning. The second reason is to the need to capture the impact of disruptions on repositioning operations. As discussed earlier, such disruptions often lead to the accumulation of empty containers in terminal yards.

Assumption 2.4: Container handling costs are fixed over time and proportional to vessel capacities (as per example shown in Table 3.1).
Container handling costs in earlier studies [18], [19] were based on leg types (e.g. connecting origin-to-destination, origin-to-transhipment). Instead, this study uses a cost structure that varies by the average vessel capacity deployed on each liner service. This change allows capturing the effects of economies of scale gained by the ocean carriers on trade lanes where larger vessels are deployed.

The use of container handling costs based on vessel capacity also reduces the pre-processing of legs parameters in larger network instances as the container handling costs do not vary in accordance to flow assignment between port pairs (leg types) but rather on the characteristics of the liner services connecting them. Container handling costs for each vessel class (shown in Table 3.1) are computed dividing time charter (TC) rates by the vessel's TEU carrying capacity defined in Brouer et al. [21]. TC rates in the case study network are also obtained from LL12 and include operating expenses (OPEX), crew and maintenance costs [21].

Assumption 2.5: Container handling costs based on vessel capacity are assumed not to vary based on the utilisation of the vessels.
We do not regard this assumption to have a fundamentally adverse effect on the quality of our analysis, as vessel utilisation would have already been considered as part of liner shipping network design. The above argument is supported by the fact that CAM implementations in this study are carried on a network built from publicly available liner service data which captures port call sequences from actual ocean carriers that design their network considering acceptable vessel utilisation levels.

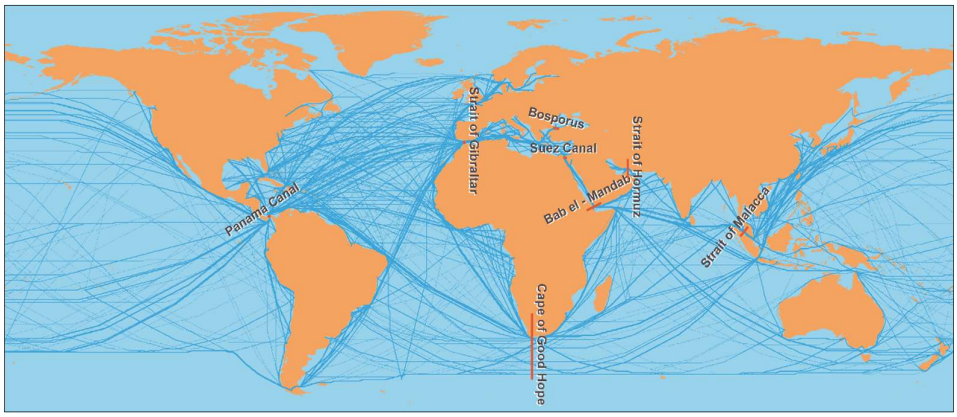

Figure 2.1**: Liner shipping services and main maritime logistics corridors (in red) source: Achurra-Gonzalez et al.** [2]

This study adopts the CAM notation introduced in [18], where + and ++ are used to simplify two reoccurring summations: $x_{a+}^{f} = \sum_{s \in D} x_{as}^{f}$ and $w_{++}^{f} = \sum_{r \in O} \sum_{s \in D} w_{rs}^{f}$.
Table **2.1** summarises the notation used in this paper, followed by the model formation.

Table 2.1: CAM and ADM notation

Sets		Subsets		Indices	
A	All legs	A_k^+	Legs entering port k	a	Legs
K	All ports	A_k^-	Legs leaving port k	k	Ports
D	Destination ports	A_n	Legs on service n	y	Corridors
O	Origin ports	L_y	Links on corridor y	l	Links
Y	All corridors	L_n	Links on service n	n	Liner services
L	All links			r	Origin ports
N	All liner services			s	Destination ports
J	Disrupted components			j	Disruption strategies
I	Defended components			i	Defence strategies
				f	Loaded containers
				e	Empty containers

Parameters	
B_k^f	Net flow of loaded containers at each port k
B_k^e	Net flow of empty containers at each port k
C_a	Sailing time on leg a, including loading and unloading times at ports (e.g. days)
CHC_{an}	Container handling cost per loaded container on leg a using liner service n
CR	Rental cost per unit time per loaded or empty containers
TD_{rs}^f	Demand of loaded containers to be transported from origin r to destination s in the defined planning horizon
TD_{rs}^e	Demand of empty containers to be transported from origin r to destination s in the defined planning horizon
DV	Depreciation cost per unit time per loaded container (inventory cost)
τ_{aln}	1 if leg a uses link l on liner service n, and 0 otherwise
τ_{aly}	1 if leg a uses link l on maritime corridor y, and 0 otherwise
F_a	Frequency of sailing on leg a
PT_k	Throughput capacity of port k
LS_n	Throughput capacity of liner service n
MC_y	Throughput capacity of maritime corridor y
δ_i	Defender flow diversion percentage in strategy i (please refer to section 4.2)
α_j	Attacker disruption percentage in strategy j (please refer to section 4.2)
$\hat{\delta}_i$	Defender capacity multiplier for network components with flow diversion in strategy i
$\hat{\alpha}_j$	Attacker capacity multiplier for disrupted network components in strategy j
PC^f	Penalty cost for loaded containers not transported
PC^e	Penalty cost for empty containers not transported

Decision variables	
t_{rs}^f	Serviced demand of loaded containers shipped from origin r to destination s
t_{rs}^e	Serviced demand of empty containers shipped from origin r to destination s
x_{as}^f	Flow of loaded containers on leg a en route to destination s
x_{as}^e	Flow of empty containers on leg a en route to destination s
w_{ks}^f	Expected dwell time at port k for all loaded containers en route to destination s
w_{ks}^e	Expected dwell time at port k for all empty containers en route to destination s
p_i	Probability defender diverts flows from component i
q_j	Probability attacker disrupts component j
z	Value of the game for the attacker (disruption costs)
v	Value of the game for the defender (routing costs)

Objective:

$$min\ Uij = \sum_{n\in N}\sum_{a\in A} CHC_{an}\left(x^f_{a+} + x^e_{a+}\right) + \left(\sum_{a\in A} x^f_{a+}C_a + w^f_{++}\right)(CR + DV) + \left(\sum_{a\in A} x^e_{a+}C_a + w^e_{++}\right)(CR) + \sum_{r\in O}\sum_{s\in D}(TD^f_{rs} - t^f_{rs})PC^f + \sum_{r\in O}\sum_{s\in D}(TD^e_{rs} - t^e_{rs})PC^e \quad (2.1)$$

Subject to:

$$\sum_{a\in A^+_k} x^f_{as} - \sum_{a\in A^-_k} x^f_{as} = B^f_k \quad \forall k \in K, s \in D \quad (2.2)$$

$$\sum_{a\in A^+_k} x^e_{as} - \sum_{a\in A^-_k} x^e_{as} = B^e_k \quad \forall k \in K, s \in D \quad (2.3)$$

$$B^f_k = \begin{cases} -\sum_{s\in D} t^f_{rs} & if\ k = r \in O \\ \sum_{r\in O} t^f_{rs} & if\ k = s \in D \\ 0 & otherwise \end{cases} \quad (2.4)$$

$$B^e_k = \begin{cases} -\sum_{s\in D} t^f_{rs} & if\ k = r \in O \\ \sum_{r\in O} t^f_{rs} & if\ k = s \in D \\ 0 & otherwise \end{cases} \quad (2.5)$$

$$x^f_{as} \le w^f_{ks}F_a \quad \forall a \in A^-_k, k \ne s \in K, s \in D \quad (2.6)$$

$$x^e_{as} \le w^e_{ks}F_a \quad \forall a \in A^-_k, k \ne s \in K, s \in D \quad (2.7)$$

$$LS_n \ge \sum_{a\in A}(x^f_{a+} + x^e_{a+})\tau_{aln} \quad \forall l \in L_n, n \in N \quad (2.8)$$

$$\hat{\alpha}_{jy}\hat{\delta}_{iy}MC_y \ge \sum_{a\in A}(x^f_{a+} + x^e_{a+})\tau_{aly} \quad \forall \in L_y, y \in Y, i \in I, j \in J \quad (2.9)$$

$$\hat{\alpha}_{jk}\hat{\delta}_{ik}PT_k \ge \sum_{a\in A^-_k}(x^f_{a+} + x^e_{a+}) + \sum_{a\in A^+_k}(x^f_{a+} + x^e_{a+}) \quad \forall k \in K, i \in I, j \in J \quad (2.10)$$

$$t^f_{rs} \le TD^f_{rs} \quad \forall r \in O, s \in D \quad (2.11)$$

$$t^e_{rs} \le TD^e_{rs} \quad \forall r \in O, s \in D \quad (2.12)$$

$$x^f_{as}, x^e_{as} \ge 0 \quad \forall a \in A, s \in D \quad (2.13)$$

The objective function (2.1) minimises the sum of network routing costs U_{ij} when cargo flow is diverted from component i by the defender and component j is disrupted by the attacker. Network routing costs cover container handling, inventory, and rental fees generated from the assignment of container flows to legs and penalty costs for containers not transported.

Constraints (2.2) through (2.5) enforce flow conservation. Constraints (2.6) and (2.7) ensure that the dwell time of loaded and empty containers is not less than the inverse of the combined liner service frequencies for the corresponding route. The capacity constraint for each liner services is defined in (2.8). Constraints for maritime corridor capacity (e.g. canals, access channels and straits) are defined in (2.9) where $\hat{\alpha}_j$ and $\hat{\delta}_i$ define the percentage of available functional capacity in attacker strategy j and defender strategy i respectively. Similarly, port throughput constraints are defined in (2.10). Detailed descriptions of the capacity multipliers for each of the players' strategies are presented in the following section. Constraints (2.11) and (2.12) ensure that the total number of full and empty containers does not exceed the demand specified in OD matrices. In

cases where network capacity falls below the total demand, the model can decide not to fulfil a portion of the demand, subject to penalties. Finally, (2.13) ensures that all flow variables are non-negative.

For the calculation of liner service capacities LS_n we adopt the approach described in Lam and Yap [22], with a weekly or monthly capacity window (instead of the originally considered annual basis). The implementation of the model (provided below) assumes that ocean carriers can determine the number of vessels to be deployed on each liner service *n* dividing the total voyage time (expressed in days) by the desired service frequency. This assumption follows from the standard industry practice to aim for weekly frequencies in most major routes, facilitated by an appropriately allocated fleet (i.e. 8 vessels for a 56 day rotation).

For services that do not operate on a weekly basis, we use effective route capacity LS_n formula provided below (2.14), determined as the multiple of average nominal vessel capacities, desired model time window and the inverse of the liner service port call frequency:

$$LS_n = \left(\frac{\sum_{h \in H_n} NC_{hn}}{TH_n}\right)\left(\frac{SMF}{F_n}\right) \quad \forall n \in N \tag{2.14}$$

Where

$n \in N$	Set of liner services in the network
$h \in H_n$	Set of container vessels deployed in liner service $n \in N$
F_n	Port call frequency of liner service $n \in N$
NC_{hn}	Nominal capacity (TEU) of container vessel $h \in H_n$ deployed in liner service $n \in N$
TH_n	Total number of vessels deployed in liner service $n \in N$
SMF	Standardised model service frequency (e.g. weekly, monthly, annual)

SMF is expressed as the actual number of days for the desired time window in which the liner service capacities will be standardised. Liner service port call frequencies F_n can be given in the input network data or replaced by $\left(\frac{VT_n}{TH_n}\right)$ where VT_n represents the total voyage time to complete a full rotation in liner service n.

2.2 Attacker-defender model (ADM)

Using the above model, we develop an attacker-defender model that can identify the most critical network components. This is formulated as a two-player, zero-sum, mixed-strategy game between a malevolent agent (attacker) and a global network operator (defender) where each player tries to optimise its utility. The game is played simultaneously, and both players have perfect information on the abilities of their opponent but no knowledge of their adopted strategy. It is used to identify a mixed-strategy Nash equilibrium with respective network disruption and routing costs for both players [23] as well as attack probabilities which represent the likelihood that the attacker will disrupt each network component. The game can be used to capture unexpected sources of disruptions with no historical precedent [7], which in this case could include recent events, such as Hanjin's bankruptcy in 2016 and Maersk's cyber-attack in 2017 [24]. Incidents of this nature can have a much more significant impact in the shipping industry than others for which action plans are already established (e.g. an earthquake or operational accidents).

In our formulation, the attacker represents an abstract entity that encompasses all potential sources of random or targeted disruption that may affect a liner shipping network. These include, but are not limited to, accidents, labour strikes, equipment failure, natural disasters, political conflicts, and terrorist attacks. The attacker's objective is to disrupt critical components and maximise disruption costs to the defender. We assume that the defender is a global ocean carrier or alliance seeking to meet transport demands in the market at the lowest possible routing cost while avoiding links or nodes disrupted by the attacker. Thus, the defender's objective is to identify any critical components that the attacker would be likely to disrupt and divert container flows in a way that minimises disruption-related rerouting and penalty costs. The payoff matrix of utilities for the two-player game is generated using the assignment model formulated in section 2.1.1, executed for all combinations of available strategies. The format of the payoff matrix and combination of potential scenarios are presented in Table 2.2.

Assumption 2.6: The attacker can disrupt only one network component at any time.
This assumption relates to the practicality of model deployment. The disruption of multiple components provides insights on component interdependencies and other aspects of systemic vulnerability. However, the number of CAM iterations required to populate a payoff matrix would increase based on the number of potential component combinations and disruption levels to be evaluated.

We address the evaluation of simultaneous disruptions with a sequential algorithm of network interventions (explained in section 2.3) that takes a payoff matrix of single disruption scenarios and iterates through the most critical components of each ADM solution instance. The result of the algorithm is a criticality ranking of network components that can be interpreted as the combination of components that would maximise the network vulnerability. This approach minimises the number of iterations required while generating sufficiently detailed outputs.

Assumption 2.7: The defender has the option to redirect cargo flows through alternative routes.
This assumption models the response of a typical ocean carrier to network disruptions where vessels can skip disrupted network components or tranship cargo flows through secondary routes with available capacity.

Assumption 2.8: The attacker can only disrupt the same set of components that the defender may choose to divert flow from ($I = J$).
This allows partial application of the approach to specific parts of the network (e.g. Northwest Europe, as in section 3). If the attacker could disrupt network components that the defender could not choose to divert flow from, the defender would not have been able to minimise the impact of disruptions from the choices of its available strategy set.

A scenario is denoted by U_{ij}, where i is the component from which the defender diverts cargo and j is the component disrupted by the attacker. With the assumptions stated above and m being the total number of elements in the sets $I = J$, the following two cases are possible for each scenario [23]:

1) Case $i = j$: The attacker and defender choose the same component to disrupt or defend, and there remain $m - 1$ components in the network that are not affected by disruption or flow diversion.
2) Case $i \neq j$: The attacker and defender choose different components to disrupt or defend, and there remain $m - 2$ unaffected components.

Using the network routing costs U_{ij} for all possible scenarios, we construct an *m*-by-*n* square matrix to serve as the payoff matrix for the game, shown in Table 2.2. The diagonal values represent scenarios where the defender predicts accurately the component that is to be disrupted by the attacker.

Table 2.2: Payoff matrix format

	Strategy j: Attacker disrupts component $j \in J$				
Strategy i: Defender diverts flows from component $i \in I$	Network Components	1	2	...	n
	1	U_{11}	U_{12}	…	U_{1n}
	2	U_{21}	U_{22}	…	U_{2n}
	...	...	…	…	…
	m	U_{m1}	U_{m2}	…	U_{mn}

U_{ij} values of the payoff matrix are populated using iterations of the CAM. The minimum number of required CAM iterations to complete the payoff matrix varies depends upon the defender flow diversion percentage δ_i and the attacker capacity disruption percentage α_j as defined in following two cases:

1) Case $\alpha_j = \delta_i$: If the attacker disruption percentage α_j equals defender flow diversion percentage δ_i, then $U_{ij} = U_{ji}$. Therefore, the minimum number of required CAM iterations increases polynomially according

to $(m+1)m/2$, which corresponds to the size the payoff matrix upper or lower triangle. In this study, values of the upper triangle payoff matrix are computed first and then assigned to corresponding components of the lower triangle.

2) Case $\alpha_j \neq \delta_i$: If the attacker disruption percentage α_j is not equal to the defender flow diversion percentage δ_i, then $U_{ij} \neq U_{ji}$. Therefore, the minimum number of required CAM iterations increases exponentially according to m^2 corresponding to the total number of elements in the payoff matrix.

These are used to define the functional capacity scalars $\hat{\alpha}_j$ and $\hat{\delta}_i$ for network components in CAM iterations required to generate network routing costs for each U_{ij} scenario in the payoff matrix. For the defender, the scalar $\hat{\delta}_i = 1 - \delta_i$ defines the functional capacity for network components with flow diversion in strategy i. Similarly, for the attacker, the scalar $\hat{\alpha}_j = 1 - \alpha_j$ defines the functional capacity for network components affected by disruptions in attacker strategy j. These relationships are summarised in Table 2.3.

Table 2.3: ADM player's strategies and network component capacity scalars

Player	Strategy	Action	Network capacity scalar
Attacker	J	Disrupt network component j by α_j	$\hat{\alpha}_j = 1 - \alpha_j$
Defender	I	Divert flow from network component i by δ_i	$\hat{\delta}_i = 1 - \delta_i$

Using the above definitions, we develop the following maximin formulation for the attacker-defender model:

Objective:

$$\max_{q_j} \left(\min_{p_i} \sum_{i \in I} \sum_{j \in J} p_i \, U_{ij} q_j \right) \tag{2.15}$$

Subject to:

$$\sum_{j \in J} q_j = 1 \tag{2.16}$$

$$\sum_{i \in I} p_i = 1 \tag{2.17}$$

$$q_j, p_i \geq 0 \quad \forall i \in I, j \in J \tag{2.18}$$

The objective (2.15) is for the attacker to maximise the expected disruption cost while the defender minimises the expected disruption cost. The constraints (2.16) through (2.18) ensure valid mixed strategies where each player assigns a probability to each component in $I = J$ such that sum of probabilities equals to one. To solve this model, we proceed to transform it into a linear formulation by introducing a variable z representing the network disruption costs and, therefore, the value of the game for the attacker.

The resulting objective (2.19) represents the attacker's intention to maximise z. Setting z on the right-hand side of the inequality constraints (2.20) ensures that the optimal strategy of the defender is taken into account because the payoff for the attacker cannot exceed the smallest expected disruption costs considering all possible moves of the defender.

Objective:

$$\max z \tag{2.19}$$

Subject to:

$$\sum_{j \in J} U_{ij} q_j \geq z \quad \forall i \in I \tag{2.20}$$

$$\sum_{j \in J} q_j = 1 \tag{2.21}$$

$$q_j \geq 0 \quad \forall j \in J \tag{2.22}$$

To derive the optimisation problem of the defender, we introduce a variable v to represent total routing costs, alongside a minimisation objective (2.23):

Objective:

$$min\ v \tag{2.23}$$

Subject to:

$$\sum_{i \in I} U_{ij} p_i \leq v \quad \forall j \in J \tag{2.24}$$

$$\sum_{i \in I} p_i = 1 \tag{2.25}$$

$$p_i \geq 0 \quad \forall i \in I \tag{2.26}$$

The model formulation for attacker strategies is the dual of the defender strategy model and vice versa. Therefore, the optimal solution would satisfy $z = v$ and the solution would be a Nash equilibrium with mixed strategies. Here, the attacker's strategy represents the worst case attack probabilities assuming that these are anticipated by the defender [25]. In other words, higher component attack probabilities would have a more adverse effect to the networks. On the other hand, the equilibrium strategy of the defender indicates the safest path choice frequency. As expected for maritime supply chain networks, this path choice frequency often involves the use of more than one path.

Bell et al. [7] point out that a particular disruption cost can be expected irrespective of the routing paths selected by the defender. Therefore, the value of the game also represents a measure of the overall vulnerability of the transport network. On the other hand, the value of the game for the defender indicates the worst-case routing costs. The routing strategy selected by the defender guarantees that regardless of attack strategies, the total routing costs will not be higher than the value of the game.

2.3 Model integration and implementation

The two models are combined to evaluate a series of iterative network interventions to generate a criticality ranking of network components. This follows from Sullivan et al. [13], who investigated the use sequential approaches to assess the relative importance of disrupted components as part of a solution procedure. This approach does not focus on the investigation of specific impacts of a single disruptive action but rather the performance of the system against known or unknown sources of disruption.

The overall workflow of the framework and the interactions between the two models are illustrated in Figure 2.2. The CPLEX engine is used to solve problem instances for the CAM model (implemented using the OPL modelling language), which are generated by the ADM (implemented using MATLAB and OPL/CPLEX). In our proposed sequential interventions, the network component with highest attack probability on each iteration t is defended against any level of disruption in iteration $t + 1$. The iterations end when all network components are defended.

Model outputs include a series network disruption costs z^* ranging from a worst-case disruption scenario (where the most vulnerable component is disrupted) to the best-case scenario (where the attacker is only able to disrupt the component with minimum network impact). Also provided are network component rankings with respect to the attack probabilities in the network. Numerical implementations of this algorithm are presented in section 3.

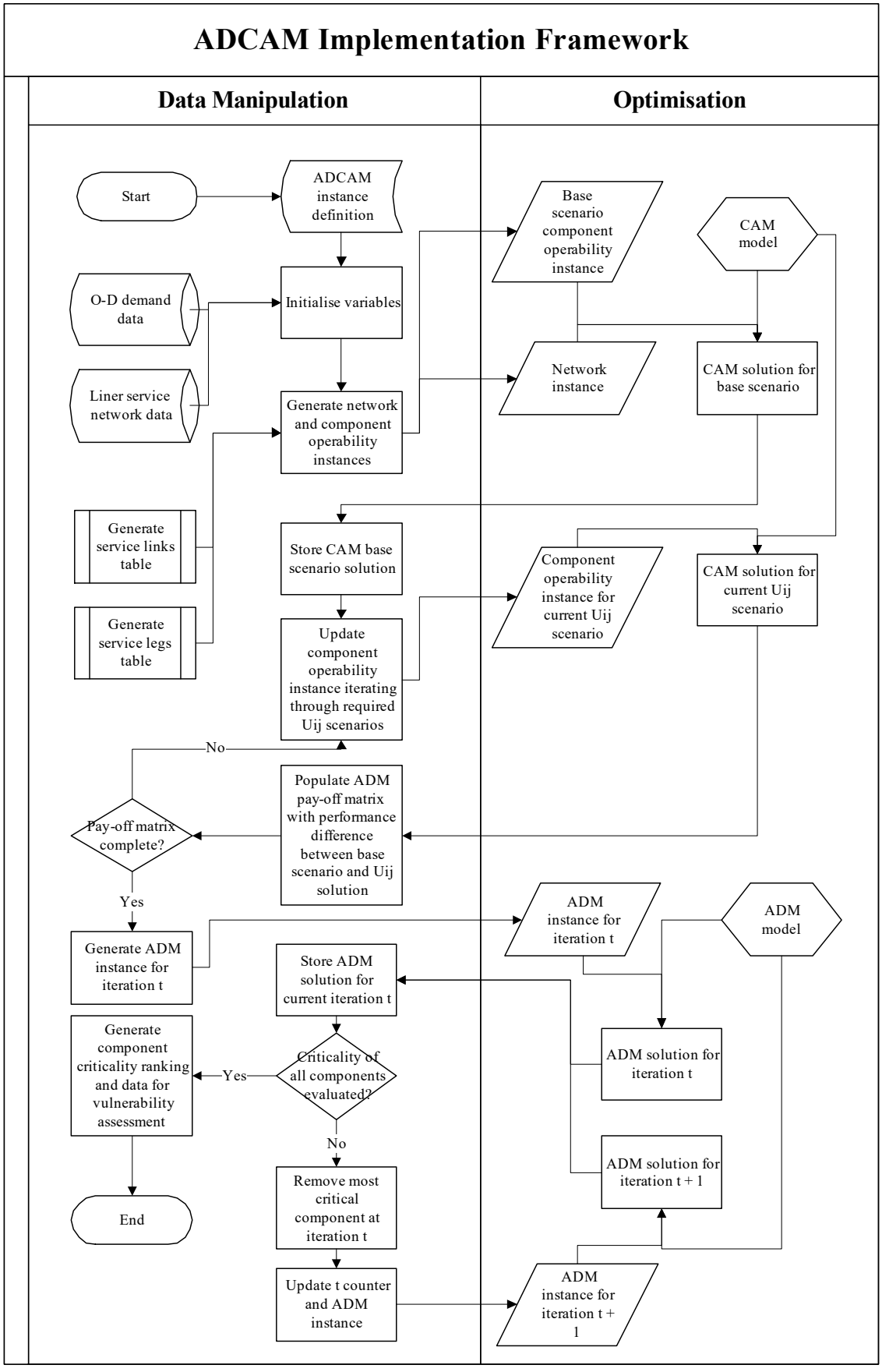

Figure 2.2: ADCAM implementation framework.

3 Numerical Analysis

In this section we describe a numerical case study using the proposed ADCAM framework. Our implementation aims to assess the systemic vulnerability of liner service networks against disruptions and to identify its most critical network components. We analyse a network-based representation of Europe's major container ports (network nodes) in terms of containerised throughput. The network is built using liner service data from a large ocean carrier and encompasses 88 distinct liner services, 230 container ports, and 2,648 OD pairs representing 242,214 weekly container movements.

3.1 Model Inputs

As market demand data for container transport services are considered by shipping lines to be commercially sensitive and central to their market strategies, we based our analysis to the LINER-LIB-2012 (LL12) dataset developed by Brouer et al. [21]. This was initially intended for use as a benchmark dataset for liner shipping network design algorithms. However, as it was developed in close co-operation with Maersk and other stakeholders in the liner shipping community, it has been deemed to be sufficiently representative for use in a broader spectrum of liner shipping studies.

A network model of the global container shipping market was created using a snapshot of the service schedules that were in effect during May 2014. This included port call rotations, transit times and nominal vessel capacities. Sources for this data include the public websites of container shipping lines, online. To maximise alignment with demand data, we also based our network dataset on services offered by Maersk. The demand for loaded containers between OD pairs used in this chapter was obtained from LL12's World Small instance whereas the number of empty containers to be repositioned corresponds to 20.5% of the loaded container demand as estimated by Rodrigue et al. [26].

We use the same costs for container rental and cargo depreciation costs as earlier studies on container assignment [18], [19]. Given the presence of economies of scale in container shipping, we define container handling costs as the ratio of time charter rates against the average TEU capacity of each vessel class. This is an improvement upon earlier studies on container assignment, which mostly used a constant value across the entire network. Cost rates were also obtained from the LL12 dataset, and incorporate operating expenses, crew salaries and maintenance costs. For this study, we assume that these do not depend upon vessel utilisation, which would have been considered during service design.

Table 3.1: Case study network parameters

Network particulars	
Depreciation rate for container cargo	80 USD/TEU/day
Undelivered container penalty (loaded)	50,000 USD/TEU
Undelivered container penalty (empty)	5,000 USD/TEU
Rental cost for loaded/empty containers	18 USD/TEU/day

Transport cost per vessel class			
Vessel class	**Capacity (TEU)**	**Time charter (USD/day)**	**Handling cost (USD/TEU/day)**
Feeder_450	900	4,680	5.20
Feeder_800	1,600	7,966	4.98
Panamax_1200	2,400	11,683	4.86
Panamax_2400	4,800	21,774	4.53
Post_Panamax	8,400	33,922	4.04
Super_PostPanamax	15,000	48,750	3.25

As a proof of concept, we concentrated our disruption analysis on the Top 6 European ports in terms of throughput as reported in Containerisation International (CI) 2012. These were in Northwest Europe and are recognised as major trade gateways for the region, with significant transhipment and feeder traffic. As a result, any disruption to these ports will have significant consequences to supply chains, industries and consumers throughout the European continent.

A total of 2,648 OD pairs are considered, amounting to 242,214 weekly TEU container movements. Table 3.1 provides a summary of the parameters used in the case study network. The penalty rates for any full or empty container flow demands that were not satisfied were assumed to be equal to 50,000 and 5,000 USD/TEU respectively. These were chosen and calibrated to exceed any alternative routing costs across all disruption scenarios U_{ij}, therefore ensuring that cargo flows are maximised while routing capacity remains available.

Port throughput rates (TEU handled per year) were obtained from CI and were used to define the upper bound capacity values for ports in the network [27]. As these figures are aggregate and describe all container traffic regardless of carrier, we use the approach described in [2] to obtain the downscaled capacity PT_k for all 230 ports in the case study network. This corresponds to the share of port capacity that would be allocated to the subset of overall container traffic considered by our case study and is as follows:

$$PT_k = \frac{\sum_{n \in N} LS_{nk}}{\sum_{\hat{n} \in \hat{N}} LS_{\hat{n}k}} RT_k \quad \forall k \in K \tag{3.1}$$

Where:

K	Set of all ports in the case study network
$\hat{N}$	Set of all liner services in the original dataset
N	Subset of services considered by the case study
LS_{nk}, $LS_{\hat{n}k}$	Weekly capacity of liner services $n \in N$ and $\hat{n} \in \hat{N}$, calling at port $k \in K$
PT_k	Adjusted weekly throughput for port $k \in K$
RT_k	Reported weekly throughput for port $k \in K$

A transhipment incidence parameter TI_k was used to indicate the relative proportion of transhipment traffic for any port k that can be disrupted. This was determined using (3.2) and is defined as the percentage of transhipment flows from the total weekly throughput at port k in the baseline scenario (BST_k) without disruptions and flow diversions. Results for each of the ports surveyed, accompanied by their corresponding UN-LOCODE, reported throughput (RT_k) and adjusted port capacity (PT_k) provided Table 3.2.

$$TI_k = \frac{BST_k - \left(\sum_{r \in O} TD^f_{rk} + \sum_{s \in D} TD^f_{ks}\right)}{BST_k} \quad \forall k \in K \tag{3.2}$$

where:

K	Set of all ports
O	Set of origin ports
D	Set of destination ports
BST_k	Weekly baseline scenario throughput at port $k \in K$
RT_k	Reported weekly throughput of port $k \in K$
TD^f_{rk}	Weekly demand for loaded containers from $r \in O$ to port $k \in K$
TD^f_{ks}	Weekly demand for loaded containers from port $k \in K$ to destination $s \in D$
TI_k	Transhipment incidence of port k in the case study network

Table 3.2: Container ports in strategy sets *I* and *J*

Port name	Country	UNLOCODE	RT_k	PT_k	BST_k	TI_k
Antwerp	BE	BEANR	162,856	27,686	5,208	68.6%
Hamburg	DE	DEHAM	151,924	12,002	2,522	15.8%
Zeebrugge	BE	BEZEE	45,960	6,342	3,214	16.6%
Bremerhaven	DE	DEBRV	93,678	54,614	28,936	34.9%
Rotterdam	NL	NLRTM	214,342	50,156	26,648	46.8%
Felixstowe	UK	GBFXT	65,384	19,812	11,146	43.7%

3.2 Model Execution

The model formulations and overall algorithm were implemented using a combination of MATLAB, the IBM OPL modelling language, and the CPLEX solver (version 12.6). Three workstations were used in parallel to minimise the time for completing the results, with Intel Xeon E5-1650, E5-2637v2, E5-2640v3 CPUs and 64, 64, 192GB RAM, respectively. As described in section Attacker-defender model , the payoff matrix for the attacker is populated with disruption costs from CAM iterations U_{ij} where the defender diverts cargo flows from network component $i \in I$ and the attacker disrupts component $j \in J$. These are defined as the difference in baseline total routing costs (without disruptions and flow diversion) and the costs on each U_{ij} scenario.

The average solution time for each CAM iteration was 17.4 minutes with a standard deviation of 1.8 minutes. As described in section Using , the number of iterations required varies by the defender flow diversion percentage δ_i and the attacker capacity disruption percentage α_j ($\alpha_j = \delta_i$ in Case 1 and $\alpha_j \neq \delta_i$ for Case 2). Section Partial disruptions describes a sensitivity analysis, carried out to evaluate how changes in disruption and flow diversion percentages may alter the vulnerability and component criticalities in the system. The disruption and flow diversion values considered range from 0% to 100% at increments of 20%.

As shown in Table 3.3, potential combinations of these disruption and flow diversion levels generate a total of 30 distinct ADCAM instances each one belonging to case 1 or 2 described above. The baseline scenario (container routing without disruptions) is the case where both α_j and δ_i would be equal to 0%.

The attacker game value z^* (in USD/week) is computed by solving the ADM model, and used as a quantitative measure of transport vulnerability of the network [25]. Also provided are the attack probabilities for each network component, indicating which ports should be targeted to maximise disruption cost and can, therefore, be considered as the most critical components of the network.

In the analysis, we consider hypothetical scenarios of iterative network interventions where the most critical port at ADM iteration $t-1$ is defended against disruptions in iteration t. The sequence at which ports are defended in this iterative approach provides a network criticality ranking for the components the attacker can disrupt at $t = 0$. The process concludes once all ports have been defended.

Table 3.3: CAM iterations for distinct combinations of α_j and δ_i

		Attacker disruption percentage					
Defender flow divert percentage	α_j / δ_i	**0%**	**20%**	**40%**	**60%**	**80%**	**100%**
	0%	Baseline	m^2	m^2	m^2	m^2	m^2
	20%	N/A	$(m+1)m/2$	m^2	m^2	m^2	m^2
	40%	N/A	m^2	$(m+1)m/2$	m^2	m^2	m^2
	60%	N/A	m^2	m^2	$(m+1)m/2$	m^2	m^2
	80%	N/A	m^2	m^2	m^2	$(m+1)m/2$	m^2
	100%	N/A	m^2	m^2	m^2	m^2	$(m+1)m/2$

3.3 Complete disruptions

In the first instance (Case 1) we considered disruptions affecting port operations, with a defender response involving the complete diversion of cargo from the ports in question ($\alpha_j = \delta_i = 100\%$). A summary of results and the resulting payoff matrix are provided in Table 4.2, which also provides an outline of intervention strategies at critical network components. Darker red values indicate higher attack probabilities and higher disruption costs. Figure 3.1 plots the changes in disruptions costs from the network interventions at the most critical port identified at $t-1$ as well as marginal financial gains from such interventions.

Total disruption costs from the most-vulnerable network state at $t = 0$ (where the most critical port is disrupted) to the least-vulnerable network state at $t = 5$ (where the attacker can only disrupt the least critical port) range from 771.5 million USD/week to 62.6 million USD/week respectively.

At $t = 0$, Bremerhaven is identified as the most critical port followed by Rotterdam with attack probabilities 0.91 and 0.09 respectively. The main reason for this result is that Bremerhaven is the port with the

largest inbound flows of containers in the OD matrix source from LL12. Furthermore, as shown in Table 6.2, the percentage of transhipment in Bremerhaven is less than Rotterdam in the case study network. Therefore, when complete disruptions occur at Bremerhaven (where $\alpha_j = \delta_i = 100\%$), more containers are unable to be transported to their final destination, resulting in higher disruption impacts. Given that most of the attack probabilities are concentrated on a single network component (Bremerhaven), the performance of the case study network is highly vulnerable to disruptions in this port.

As part of the network intervention scenarios, at $t = 1$, Bremerhaven is defended against disruptions for being the port with highest attack probabilities at $t = 0$. Resulting financial gains from this intervention are USD 89 million/week (-11.6% marginal disruption cost z^* decrease). An exclusion of Bremerhaven from the set of ports that the attacker can disrupt is found to have a significant effect on the attack probabilities of other ports. The updated attack probabilities identify Rotterdam as the new most critical port followed by Felixstowe with attack probability values of 0.90 and 0.10 respectively. The updated attack probabilities are still clearly concentrated at Rotterdam, which represents a singular point of vulnerability for the network as modelled.

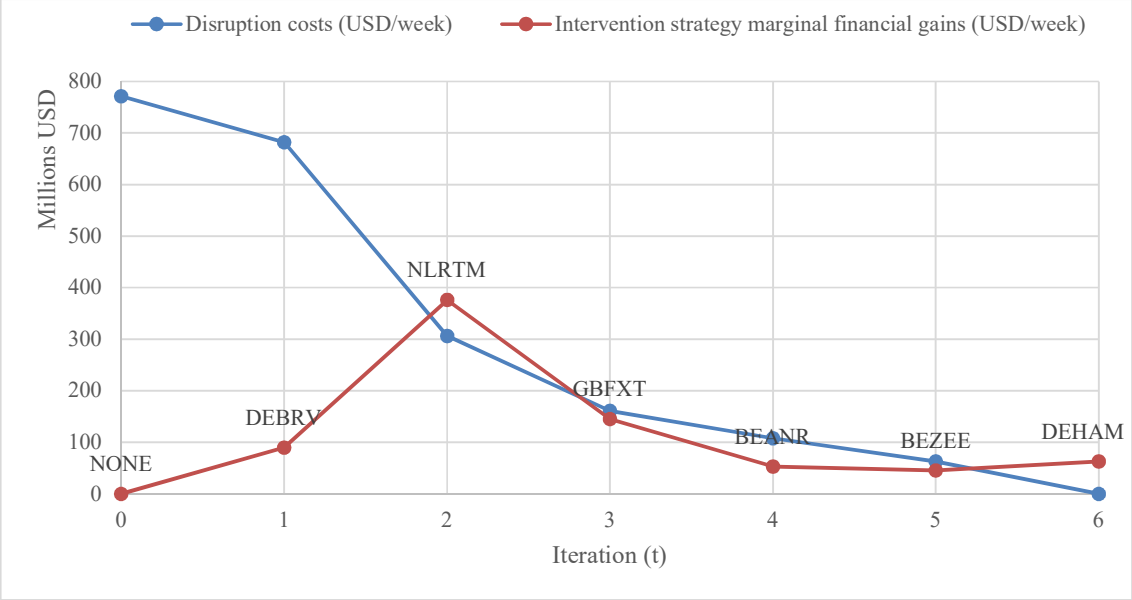

Figure 3.1: Disruption costs and intervention financial gains.

At $t = 2$, Rotterdam is defended against disruptions. This intervention produces a dramatic decrease in disruption costs z^* (-48.7%) resulting in 376 million USD/week in marginal financial gains from defending the port of Bremerhaven and Rotterdam in tandem. This intervention represents the largest financial gain from including a port in the set of the defended components. Updated attack probabilities are 0.77 for Felixstowe and 0.23 for Antwerp. Though the attack probabilities are still mostly concentrated on two ports, they start to spread more across network components (when compared to previous iterations) making it difficult for the attacker to maximise disruption costs from disabling a single port in the network.

At $t = 3$, Felixstowe is defended against disruptions. This intervention produces the second largest financial gain: USD 145.3 million/week (-18.8% marginal z^* decrease). Updated attack probabilities are for the first time spread amongst 3 ports: 0.57 for Antwerp, 0.31 for Zeebrugge, and 0.12 for Hamburg. Therefore, upon removing Bremerhaven, Rotterdam and Felixstowe from the set of the ports the attacker can disrupt, the choice of a single port to disrupt to maximise disruption costs is less clear for the attacker. These results suggest that the Bremerhaven, Rotterdam, and Felixstowe are the most critical ports in the case study network.

At $t = 4$, Antwerp is defended against disruptions resulting in financial gains of 52.8 million USD/week (-5.9% marginal z^* decrease). Updated attack probabilities for the two remaining ports are almost equivalent with 0.56 for Zeebrugge and 0.44 for Hamburg. Iterations $t = 5$ and $t = 6$ defend Zeebrugge and Hamburg respectively with combined financial gains of 107 million USD/week.

The sequence at which ports are defended through this iterative approach provides a network criticality ranking for the components the attacker can disrupt at $t = 0$. Figure 3.2 presents a geographical representation

of the case study ports color-coded based on their network criticality ranking (where lower values indicated higher criticality). The size of the ports represents the total network disruption costs z^* that the attacker can achieve when disrupting each port.

3.4 Partial disruptions

This section describes the sensitivity analysis that evaluates how changes in disruption (α_j) and flow diversion (δ_i) influence network vulnerability and criticality ranking of the selected ports. We evaluated disruption and flow diversion levels between the range of 0% to 100% at increments of 20%, in 30 distinct network instances (described in Table 3.3). Figure 4.3 presents the changes in network disruption costs z^* and the changes in criticality rankings.

For disruption levels $\alpha_j \leq 20\%$, Felixstowe is the most critical port in the network with disruption costs ranging from 70.5 thousand USD/week (at defender flow diversion $\delta_i = 0\%$) up to 62.74 million USD/week (at $\delta_i = 100\%$). At this disruption level, Rotterdam is the second most critical port followed by Bremerhaven. Disruptions costs at Rotterdam are very close to those in Felixstowe ranging from 65.3 thousand USD/week at $\delta_i = 0\%$ up to 62.73 million USD/Week at $\delta_i = 100\%$.

For Bremerhaven, disruption costs at $\alpha_j \leq 20\%$ are lower when the defender does not divert any cargo flow (327 USD/week at $\delta_i = 0\%$ up to 62.67 million USD/Week at $\delta_i = 100\%$). This suggests that in the case study network, Felixstowe and Rotterdam have less spare capacity to withstand disruptions lower than 20% when compared to Bremerhaven.

As shown in Figure 3.3, the criticality ranking of remaining ports in the network for $\alpha_j \leq 20\%$ is Antwerp (4th most critical), Zeebrugge (5th most critical), and Hamburg (6th most critical). Disruptions costs range from 0 USD/week when the defender does not divert any cargo flows ($\delta_i = 0\%$) but increase to 62.6 million USD/week when the defender deviates all cargo flows to other terminals ($\delta_i = 100\%$).

For disruption levels α_j between 20% and 40%, Felixstowe remains the most critical port in the network with costs between 3.3 million USD/week (at $\delta_i = 0\%$) and 65.9 million USD/week (at $\delta_i = 100\%$). For this interval, Bremerhaven becomes the second most critical port surpassing Rotterdam. For these two ports, disruptions costs range from 1.5 million USD/week (at $\delta_i = 0\%$) up to 64.5 million USD/week at $\delta_i = 100\%$. The criticality ranking of Antwerp, Zeebrugge remain unchanged at this disruption interval.

For the remaining ADCAM instances with disruption levels α_j greater than 60%, Bremerhaven becomes the most critical port of the network with disruption costs up to 771.5 million USD/Week ($\alpha_j = 100\%, \delta_i = 100\%$). Rotterdam remains as the second most critical port in the network with disruption costs up to 682.2 million USD/week whereas Felixstowe falls to the third position with disruption costs of up to 306.1 million USD/week. For disruption levels of 100%, Antwerp, Zeebrugge, and Hamburg stabilise on the 4th, 5th, and 6th critical rank respectively.

3.5 Discussion

The changes in criticality ranking of ports and overall disruption costs are primarily driven by the available spare capacity that each port has to meet its inbound and outbound throughput as well as any transhipment cargo flows. Since Felixstowe operates with lower spare capacity, it is more susceptible to lower disruptions levels (e.g. $\alpha_j \leq 40\%$) when compared with Rotterdam and Bremerhaven. As such, it is the most critical port for lower disruption levels.

In contrast, Bremerhaven and Rotterdam, which operate with more spare capacity, are capable of withstanding disruption levels below 40% without significantly increasing the overall network disruption costs. However, these ports surpass Felixstowe in the criticality ranking for disruptions levels above 60% due to the more significant number of containers affected when disruptions occur at Bremerhaven or Rotterdam.

These results are significantly influenced by the OD matrix input where most container flows are destined to Bremerhaven, Rotterdam, and Felixstowe. Consequently, disruptions in Antwerp, Zeebrugge, and

Hamburg have less impact on the overall network vulnerability. The latter ports have lower inbound and outbound flows in the case study network (between 2.5 and 5.2 thousand TEU/week).

In the case study network, ports such as Antwerp have high transhipment incidence in the baseline scenario (about 69%) and therefore can be replaced with secondary paths when cargo flows cannot be routed through this port. On the contrary, Bremerhaven, Rotterdam, and Felixstowe have the characteristic feature of high inbound and outbound flows (between 18 and 50 thousand TEU/week) as well as lower transhipment incidence in the case study network (between 35% and 47%). As such, interventions that prevent disruptions at the latter ports result in higher financial gains across the ADCAM instances evaluated.

The sensitivity analysis also demonstrates that the defender strategy of deviating cargo flows does not reduce the vulnerability of the case study network. Instead, the iterative interventions that protect network components and rank port criticality proved beneficial in reducing the network vulnerability. This study used a divert flow strategy for the defender because in the developed two-player game, the defender is assumed to be an ocean carrier with no capacity to defend the port infrastructure but with the ability to deviate cargo flows to other ports. Therefore, future improvements to the methodology could replace defensive divert flow strategies with a network component defence strategy, which considers further potential gains from the latter approach.

Table 3.2: ADCAM results for $\alpha_j = \delta_i = 100\%$

CAM Payoff matrix disruption costs (USD/week)							
Defender: Scenarios i		Attacker: Scenarios j					
	Network Components	DEBRV	NLRTM	GBFXT	BEANR	BEZEE	DEHAM
	DEBRV	7.14E+08	1.37E+09	9.91E+08	8.41E+08	7.94E+08	7.77E+08
	NLRTM	1.37E+09	6.56E+08	9.34E+08	7.85E+08	7.36E+08	7.19E+08
	GBFXT	9.91E+08	9.34E+08	2.77E+08	4.06E+08	3.57E+08	3.40E+08
	BEANR	8.41E+08	7.85E+08	4.06E+08	1.28E+08	2.08E+08	1.91E+08
	BEZEE	7.94E+08	7.36E+08	3.57E+08	2.08E+08	8.05E+07	1.43E+08
	DEHAM	7.77E+08	7.19E+08	3.40E+08	1.91E+08	1.43E+08	6.27E+07

Attacker-Defender Model (ADM)									
t	Intervention Strategy	Disruption costs z^* (USD/week)	Marginal financial gains (USD/week)	Attack probabilities					
				DEBRV	NLRTM	GBFXT	BEANR	BEZEE	DEHAM
0	NONE	7.72E+08	-	0.91	0.09	0.00	0.00	0.00	0.00
1	DEBRV	6.82E+08	8.94E+07	0.00	0.90	0.10	0.00	0.00	0.00
2	NLRTM	3.06E+08	3.76E+08	0.00	0.00	0.77	0.23	0.00	0.00
3	GBFXT	1.61E+08	1.45E+08	0.00	0.00	0.00	0.57	0.31	0.12
4	BEANR	1.08E+08	5.29E+07	0.00	0.00	0.00	0.00	0.56	0.44
5	BEZEE	6.27E+07	4.52E+07	0.00	0.00	0.00	0.00	0.00	1.00
6	DEHAM	0.00E+00	6.27E+07	0.00	0.00	0.00	0.00	0.00	0.00

DEBRV: Bremerhaven, NLRTM: Rotterdam, GBFXT: Felixstowe, BEANR: Antwerp, BEZEE: Zeebrugge, DEHAM: Hamburg

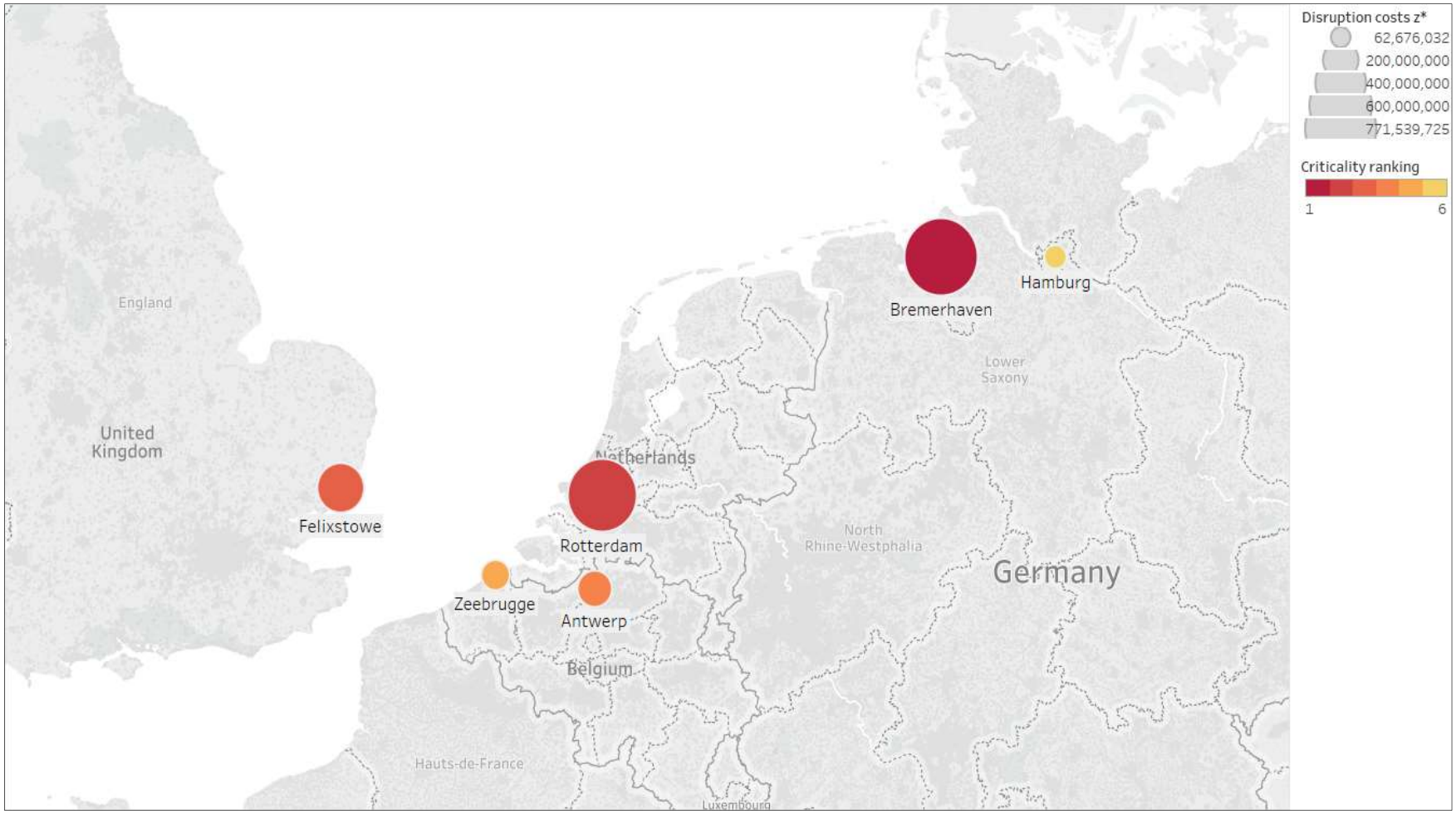

Figure 3.2: Disruption costs and component criticality ranking for $\alpha_j = \delta_i = 100\%$

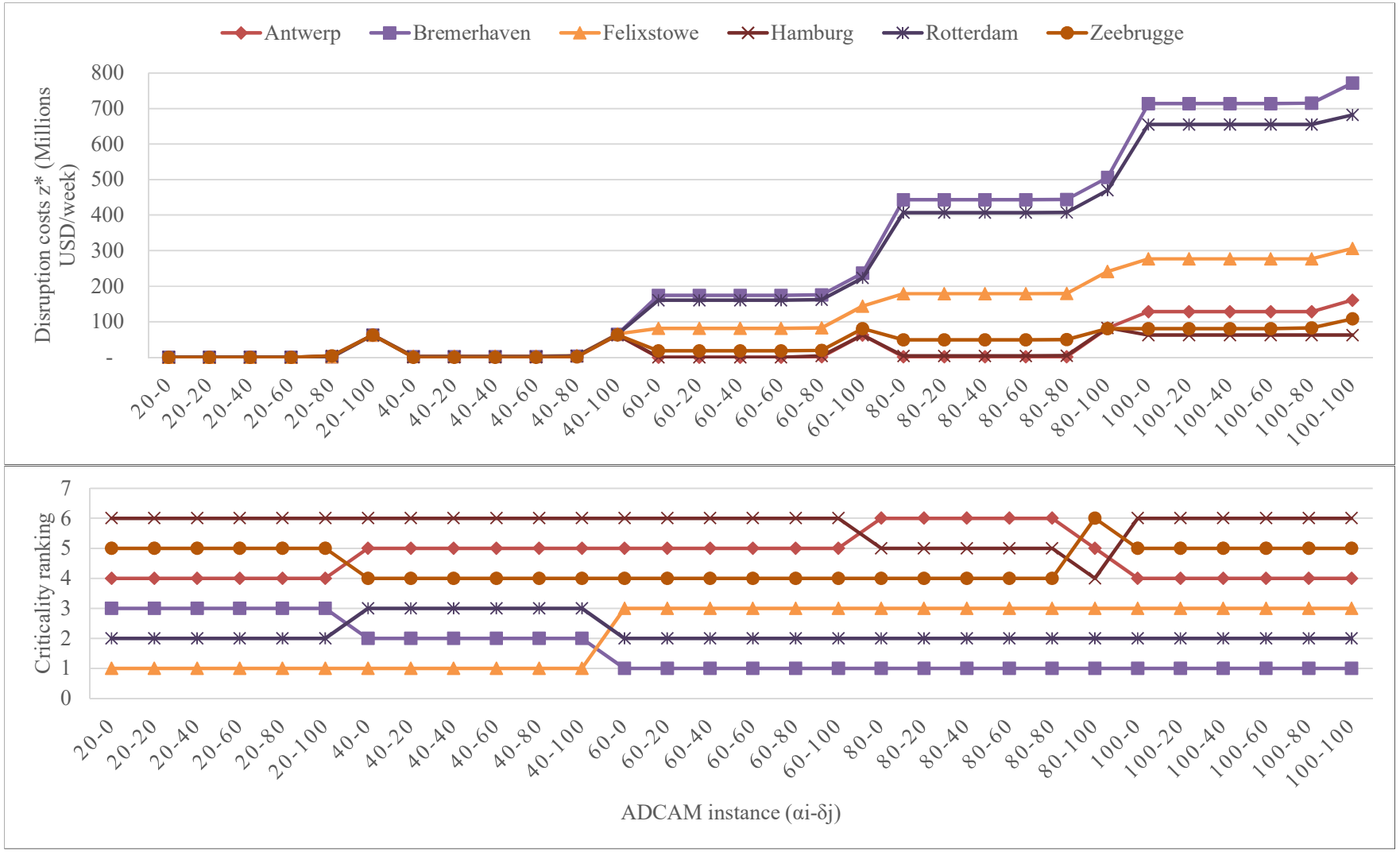

Figure 3.3: Disruptions costs and criticality rankings for all ADCAM instances

4 Conclusions and further research

This study proposes a new framework capable of identifying the most critical network components and quantifying the systemic vulnerability of realistic large-scale liner shipping networks with limited or no historical disruption data available. The case study on a subset of the European port system indicates a significant concentration of attack probabilities in specific ports, rendering the system particularly susceptible to disruption.

The network instances used in the scenarios presented in this study make extensive use of secondary data (e.g. same operating speed for all vessels and same penalty costs for all containers), leaving room for further refinements in the selection of data sources and calibration inputs. Future improvements to this framework could also include the inclusion of hinterland links, and the use of an $n + m$ player game structure where multiple carriers compete in cargo rerouting.

Another substantial enhancement to the ADM proposed in this study would be the formulation of less extreme attackers. As mentioned by Bell et al. [7], a logit model approach can be used to adjust the level of aggressiveness of attackers (or user pessimism) that a particular network component will fail in the network evaluated. This approach allows departure from worst-case scenario analysis resulting from the formulation of extremely aggressive attackers or pessimistic users (as presented in this study) and provide a vulnerability assessment of transport networks exposed to less extreme events which are more common in liner shipping.

Finally, the interventions proposed by this study assume that it is possible to make centralised decisions on network structure when aiming to reduce exposure to disruptions. While this may be possible in some instances (e.g. an international financial institution allocating funds to port infrastructure in a given region), in most cases, liner shipping stakeholders would be subject to competitive tendencies. We therefore identify the relationship between market dynamics and the collective actions that contribute to collective robustness against disruption as a fertile ground for future work.

5 Acknowledgements

The authors extend their gratitude to the Georgia Tech Panama Logistics Innovation & Research Center for contributing part of the data used in this study. We also thank Professor Dongping Song, Professor Michael G. H. Bell, and colleagues at the Port Operations Research & Technology Centre of Imperial College London for their valuable feedback to previous versions of work. The corresponding author would like to thank the National Secretariat of Science Technology and Innovation of the Republic of Panama for the financial support received through research fellowship No. 2199-35-2012.

6 References

[1] UNCTAD, "Review of Maritime Transport 2017," Geneva, 2017.

[2] P. E. Achurra-Gonzalez, P. Angeloudis, K. Zavitsas, A. Niknejad, and D. J. Graham, "Attacker-defender assessment of vulnerability in maritime logistics corridors," in *Advances in Shipping Data Analysis and Modeling. Tracking and Mapping Maritime Flows in the Age of Big Data*, C. Ducruet, Ed. Routledge, 2017.

[3] W. Qiao, Y. Lu, C. Xiong, and A. Haghani, "A game theory approach for the measurement of transport network vulnerability from the system prospective," *Transp. B Transp. Dyn.*, vol. 2, no. 3, pp. 188–202, Sep. 2014.

[4] PIANC, "Resilience of the Maritime and Inland Waterborne Transport System." The World Association for Waterborne Transport Infrastructure, 2017.

[5] M. Ouyang, L. Zhao, L. Hong, and Z. Pan, "Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability," *Reliab. Eng. Syst. Saf.*, vol. 123, pp. 38–46, 2014.

[6] S. Lhomme, "Vulnerability and resilience of ports and maritime networks to cascading failures and

targetted attacks," in *Maritime networks : spatial structures and time dynamics*, C. Ducruet, Ed. Routledge, 2015.
[7] M. G. H. Bell, U. Kanturska, J.-D. Schmöcker, and A. Fonzone, "Attacker–defender models and road network vulnerability," *Philos. Trans. R. Soc. London A Math. Phys. Eng. Sci.*, vol. 366, no. 1872, pp. 1893–1906, Jun. 2008.
[8] C. Ducruet and F. Zaidi, "Maritime constellations: a complex network approach to shipping and ports," *Marit. Policy Manag.*, vol. 39, no. 2, pp. 151–168, Mar. 2012.
[9] J. A. Paul and M. J. Maloni, "Modeling the effects of port disasters," *Marit. Econ. Logist.*, vol. 12, no. 2, pp. 127–146, Jun. 2010.
[10] P. Angeloudis, K. Bichou, M. G. H. Bell, and D. Fisk, "Security and reliability of the liner container-shipping network: analysis of robustness using a complex network framework," *Risk Manag. Port Oper. Logist. Supply Chain Secur.*, pp. 95–106, 2007.
[11] C. Ducruet, S.-W. Lee, and A. K. Y. Ng, "Centrality and vulnerability in liner shipping networks: revisiting the Northeast Asian port hierarchy," *Marit. Policy Manag.*, vol. 37, no. 1, pp. 17–36, Jan. 2010.
[12] C. Ducruet, "The polarization of global container flows by interoceanic canals: geographic coverage and network vulnerability," *Marit. Policy Manag.*, vol. 43, no. 2, pp. 242–260, Feb. 2016.
[13] J. L. Sullivan, D. C. Novak, L. Aultman-Hall, and D. M. Scott, "Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: A link-based capacity-reduction approach," *Transp. Res. Part A Policy Pract.*, vol. 44, no. 5, pp. 323–336, Jun. 2010.
[14] X. Qi, "Disruption Management for Liner Shipping," in *Handbook of Ocean Container Transport Logistics: Making Global Supply Chains Effective*, C.-Y. Lee and Q. Meng, Eds. Springer International Publishing, 2015, pp. 231–249.
[15] P. E. Achurra-Gonzalez *et al.*, "Modelling the impact of liner shipping network perturbations on container cargo routing: Southeast Asia to Europe application," *Accid. Anal. Prev.*, Jun. 2016.
[16] B. D. Brouer, D. Pisinger, and S. Spoorendonk, "Liner Shipping Cargo Allocation with Repositioning of Empty Containers," *INFOR*, vol. 49, no. 2, pp. 109–124, May 2011.
[17] D.-P. Song and J.-X. Dong, "Cargo routing and empty container repositioning in multiple shipping service routes," *Transp. Res. Part B Methodol.*, vol. 46, no. 10, pp. 1556–1575, Dec. 2012.
[18] M. G. H. Bell, X. Liu, J. Rioult, and P. Angeloudis, "A cost-based maritime container assignment model," *Transp. Res. Part B Methodol.*, vol. 58, pp. 58–70, Dec. 2013.
[19] M. G. H. Bell, X. Liu, P. Angeloudis, A. Fonzone, and S. H. Hosseinloo, "A frequency-based maritime container assignment model," *Transp. Res. Part B Methodol.*, vol. 45, no. 8, pp. 1152–1161, Sep. 2011.
[20] B. Jourquin, G. Iassinovskaia, J. Lechien, and J. Pinna, "Lines and Services in a Strategic Multi-modal Freight Network Model: Methodology and Application," 2008.
[21] B. D. Brouer, J. F. Alvarez, C. E. M. Plum, D. Pisinger, and M. M. Sigurd, "A Base Integer Programming Model and Benchmark Suite for Liner-Shipping Network Design," *Transp. Sci.*, vol. 48, no. 2, pp. 281–312, 2014.
[22] J. S. L. Lam, "Patterns of maritime supply chains: slot capacity analysis," *J. Transp. Geogr.*, vol. 19, no. 2, pp. 366–374, Mar. 2011.
[23] K. Zavitsas, "The Vulnerability of the Petroleum Supply Chain," Imperial College London, 2011.
[24] J. Saul, "Global shipping feels fallout from Maersk cyber attack," *Reuters*, 2017. [Online]. Available: http://uk.reuters.com/article/us-cyber-attack-maersk-idUKKBN19K2LE. [Accessed: 07-Aug-2017].
[25] U. Kanturska and P. Angeloudis, "Introduction to network theory and game theory as frameworks for the analysis of critical infrastructure," *Inst. Eng. Technol. Infrastruct. Risk Resil. Transp.*, pp. 22–28, Jan. 2013.
[26] J.-P. Rodrigue, C. Comtois, and B. Slack, *The Geography of Transport Systems*. Routledge, 2013.
[27] Containerisation International, *Containerisation International Yearbook 2012*. London: Informa Maritime & Transport, 2012.