2022

Definition and Detection of Hypervulnerabilities Using a Framework for Assessing Port Resilience

Katherine Smith
Old Dominion University

Rafael Diaz
Old Dominion University, rdiaz@odu.edu

Yuzhong Shen
Old Dominion University, yshen@odu.edu

Francesco Longo
University of Calabria

Original Publication Citation

Smith K., Diaz R., Shen Y., and Longo F. (2022).,Definition and Detection of Hypervulnerabilities using a Framework for Assessing Port Resilience. Proceedings of the 24th International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation(HMS 2022), 002 . DOI: https://doi.org/10.46354/i3m.2022.hms.002

Proceedings of the 24th International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation (HMS), 002
19th International Multidisciplinary Modeling & Simulation Multiconference

2724-0339 © 2022 The Authors.
doi: 10.46354/i3m.2022.hms.002

Definition and Detection of Hypervulnerabilities using a Framework for Assessing Port Resilience

Katherine Smith[1,2,*], Rafael Diaz[1], Yuzhong Shen[2], and Francesco Longo[3]

[1]Virginia Modeling, Analysis & Simulation Center, Old Dominion University, 1030 University Blvd, Suffolk, VA, 23435, United States of America
[2]Department of Computational Modeling and Simulation Engineering, Old Dominion University, 1300 Engineering & Computational Sciences Building, Norfolk, VA, 23529, United States of America
[3]Mechanical Department, University of Calabria, Via Pietro Bucci, 87036 Arcavacata, Rende CS, Italy

[*]Corresponding author. Email address: k3smith@odu.edu

Abstract

Long term plans for maritime ports are identifying investments that will increase their capacity while decreasing their environmental footprint and operating costs. These changes are leading to increases in complexity at a time when leaner practices are driving investments to become more strategic. As such, this work proposes a generalized definition that allows a system or entity to be classified as exceedingly vulnerable by comparing it to other entities. This definition is developed from a set of definitions gathered from disparate fields. From this definition grounded in theory, the initial rules for complex system implementation are developed and demonstrated on both a small conceptual example and a port example. Finally, conclusions and directions for future work are provided.

Keywords: Ports; Risk analysis; Resilience; Vulnerability; Functional dependency analysis; Modeling and simulation

1. Introduction

Long term planning documents for maritime ports have identified investment in advanced equipment capability as a goal that will decrease their environmental footprint and operational costs while simultaneously increasing their container handling capacity (The Port of Virginia, 2016). These investments involve electrification, intermodal transportation, and cyber physical systems. This digitalization is one of the drivers that is making modern port operations are increasingly complex. In addition, a focus on leaner system design and operation has resulted in smaller margins of error and a push to make investments in systems where they stand to have maximum impact on system resilience. Stakeholders are consistently striving to find opportunities to optimally invest funds in the most vulnerable entities. As such, it is wise to apply some metric and list of rules so that entities can be compared to one another, and a determination made on whether one entity is more vulnerable than another. In this work, we propose a definition for an exceedingly vulnerable system entity and refer to this vulnerability as a hypervulnerability.

The remainder of this article is organized as follows:

Section 2 provides background on vulnerability as well as a short overview of the analysis methodology that will be utilized in Section 5. Section 3 provides the initial theory and definition for a hypervulnerability and its application to a small hypothetical example. Section 4 will present a case study and results showing an example application of the hypervulnerability theory using an existing framework for port resilience developed by the authors (Smith, Diaz, & Shen, 2022; Smith, Diaz, Shen, & Longo, 2021). Section 5 will conclude the paper and provide recommendations for future work.

2. State of the art

In this section, an overview of vulnerability in complex systems will be provided as well as a brief overview of the layered network dependency analysis used to implement the example in Section 4.

2.1. Vulnerability in Complex Systems

Vulnerability has varied definitions across different fields. These definitions can be perceived as conflicting. However, when carefully considered, they can be combined to build a generalized, flexible definition for vulnerability that will be extended and quantified in Section 3 of this work.

First, consider a selection of definitions for vulnerability from a variety of domains. Definitions from various technical and non-technical fields are shown in Table 1. The two main components of each of these definitions are as follows:

1. Vulnerability is described as a quality, feeling, condition, or weakness all of which are states, and
2. Vulnerability is experienced when an entity (or set of entities) is susceptible to attack, harm, uncertainty, risk, emotional, exposure, hazards (and their associated impacts), or threats.

Parts of the definitions omitted by the previous statement include: (1) particular entities (or systems) that could be affected by the vulnerability and (2) defining parameters or characteristics of those entities which increase or decrease vulnerability. These two items are domain specific and therefore will be excluded from the general definition developed and utilized in this work.

It is of interest not only to define vulnerability, but also to quantify it as a relative level of exposure to harm or threat. Therefore, the previously mentioned definitions from disparate domains should be combined into a single cohesive statement describing a quantifiable variable. Vulnerability is a quantity that describes the degree to which a system or entity is exposed to risk of disruption and its potential to be resilient to change should this disruption occur. The implication of this definition is that vulnerability can be evaluated with respect to risk, resilience, and uncertainty. Though only risk and resilience are stated in the definition, uncertainty is included implicitly as the disruption may or may not occur. Therefore, the definition can be written mathematically as follows:

$$Vulnerability = f(risk, resilience, uncertainty) \tag{1}$$

Table 1. Vulnerability definitions for various domains.

Domain	Author	Definition	Source
General	Oxford English Dictionary	"The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally."	(Oxford English Dictionary, 2021)
Human Behavior	Brené Brown	"The feeling we get during times of uncertainty, risk, or emotional exposure"	(Brown, 2019)
Disaster Recovery	United Nations Office for Risk Reduction	"The conditions determined by physical, social, economic, and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards."	(United Nations Offce for Disaster Risk Reduction, 2021)
Computer and Cybersecurity	National Institute of Standards and Technology	"Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat."	(Ross, McEvilley, & Oren, 2016)

Though the definition of vulnerability above may seem over simplified, the process of assessing and quantifying risk, resilience, and uncertainty for even a single entity can be incredibly challenging. There have been many academic studies related to determining drivers of factors and their impacts on complex systems in a variety of fields. Assessing the vulnerability of communities that are exposed to risks from natural disasters or natural hazards, such as climate change, is usually performed using vulnerability indices (Burton, 2015; Mustafa, Ahmed, Saroch, & Bell, 2011; Tate, 2012). These indices score individuals or groups to provide values for individual variables, called indicators, that are aggregated to provide a single numerical result. Due to variations in populations and no consensus on optimum processes to create indices, overall creation of these metrics is a subjective process that can be highly dependent on decisions made by developers (Tate, 2012). In the face of climate change, increasing human population, and other drivers of decreasing biodiversity, identifying vulnerabilities in the transmission of diseases from animals to humans has been under study in recent years (Charrahy et al., 2021; Pandit et al., 2018). This highlights a need to compare studies and related interventions using standardized metrics for risk, resilience, and vulnerability in order to aggregate and compare results across researchers worldwide. The COVID-19 pandemic has only highlighted the importance of accurately assessing the risks associated with this transmission and exploring ways to increase human resilience against these diseases (Platto, Wang, Zhou, & Carafoli, 2021). Establishing the difficulty and increasing importance of quantifying vulnerability across domains highlights the importance of understanding and assessing gaps in vulnerability research.

2.2. Vulnerability in Networked Systems

Modeling and simulation of vulnerability, disruption and resilience in systems modeled as networks is non-trivial for many reasons including the fact that disruptions tend to ripple through the system and cause complex interdependent failures at not only the target node, but other nodes as well (Havlin, Kenett, Bashan, Gao, & Stanley, 2014). In fact, these effects propagate forward and backward and can therefore return to the original disrupted node (Li, Chen, Collignon, & Ivanov, 2021).

Blackhurst et al. indicate that disruption discovery is critically related to supply chain visibility, capacity, and analytics (Blackhurst, Craighead, Elkins, & Handfield, 2005). In this work, the focus will be on the third item, specifically providing a definition of vulnerability to help create a set of metrics that can be used to inform models on which nodes have the highest levels of vulnerability. Some previous work has defined a disruption leading to vulnerability in a limited way such as a cessation of cargo flowing through a port for a minimum period of time (Thekdi & Santos, 2016). These works have produced promising results in risk and sensitivity analysis which indicates that further diversifying the definition of vulnerability could lead to even more promising results. Alternatively, the level of vulnerability has been linked to the topology of the network based on simulated attacks (Calatayud, Mangan, & Palacin, 2017).

2.3. Layered Network Dependency Analysis

Network dependency analysis methodology traces its origins back to Leontief Input-Output models (Leontief, 1951). These models have since been extended to assess and model risk in complex systems (Garvey & Pinto, 2009). This methodology, known as Functional Dependency Network Analysis (FDNA) represented the performance of a given system node as a piecewise, linear combination of the performance of the nodes it depended on. The next advancement introduced additional complexities in the transfer equations between nodes as well as a dependency on the internal health of the node (Guariniello & DeLaurentis, 2017).

To account for disruptions and cyclic dependencies, the authors of the current work have introduced two further enhancements. The first is two combine the overall network (for clarity referred to as the system network) of the network dependency analysis with a Bayesian network that is used to introduce disruptions that may have complex dependencies (Smith et al., 2021). The second is to partition the system network into layers in order to allow feedback between the nodes and capture complex behaviors such as ripple effects (Smith et al., 2022). This enhanced Layered network dependency analysis will be used to model the port under study so that the hypervulnerabilities can be discussed.

3. Materials and Methods

Increases in system complexity and a focus on leaner system design and operation have been seen across an array of fields. This has resulted in smaller margins of error and a push to make investments in systems where they stand to have a large, positive impact on system operation. With this in mind, system designers are not just looking to shore up resilience for any vulnerable system entity, but to invest funds in increasing resilience for the most vulnerable entities. It is prudent to apply some level of definition and scale so that a determination can be made on whether one entity is more vulnerable than another. In this section, such a definition is proposed to characterize an exceedingly vulnerable system entity and this vulnerability is referred to as a hypervulnerability.

3.1. Initial Theory

The definition of hypervulnerability is developed based in the literature on characteristics of an entity that increase its vulnerability. We propose that a system hypervulnerability is a vulnerability that demonstrates more than X of the following criteria:

1. Prevents the system from meeting at least one of its critical operational requirements.
2. Adversely effects more that Y% (or Z) system entities.
3. Effects are felt at more than A% of the initial (or maximum) impact of the disturbance for at least B months (years, day, etc.)
4. Occurs with a probability (or expectation) of at least once per month (year, day, etc.)
5. The expected cost of impact is more than (some threshold like 10% of annual gross revenue for

the company).

6. Is a combination of two individual vulnerabilities that are likely to occur together and whose effects may not combine linearly.

It is best to exercise careful consideration and consult subject matter experts when setting limits for the above criteria. However, there are cases in which the only option is to start with a best guess for these parameters. The next section will show results of choosing different parameters and provide some recommendations for analysts on choosing appropriate parameters.

It is reasonable to assume that vulnerability has an implicit scale of measurement as it is common to say one entity or feature of a system is more vulnerable than another. With this basic assumption, seeking to identify hypervulnerabilities in a system is a task in ascertaining where the vulnerability is maximum. Defining the vulnerability of node *i* is written v_i, then the index of the node where a maximum vulnerability occurs can be written:

$$argmax(v_i) \tag{2}$$

However, v_i is a function of characteristics of the potentially effected system nodes, the probability of occurrence of the risk (i.e., $P(R_i)$, and the magnitude of the effect at each effective node *j* if the risk occurs (i.e., $A_j(R_i)$) (an extension of theory from (Wagner & Neshat, 2010)). Let's assume we are discussing a risk at node i and the group of nodes affected by the occurrence of the risk event is a cluster around node *i* that we can define as V^i. Let us further define each individual node in V^i as v_j^i with a feature vector of characteristics assigned to these nodes as C_j^i . With these definitions in mind, we can write the following:

$$v_i = f\left(C_j^i, P(R_i), A_j(R_i)\right) \tag{3}$$

3.2. Hypervulnerability Thresholds

While the previous section suggests the use of the argmax function to identify the most vulnerable node, in reality, it is better to identify a set of hypervulnerable nodes. This is because the most vulnerable node may be resistant to efforts aimed at decreasing its vulnerability. In general, since the resources allocated to decrease vulnerability (and therefore increase resilience) are limited, it is prudent to apply these resources to a set of nodes in a way that optimizes the decrease in vulnerability for the entire system rather than specifically targeting the most vulnerable node.

Figure 1 shows a conceptual example of hypervulnerability thresholds. For clarity, the risk network and system network are shown separately with the dependency of nodes in the system network on particular risk nodes shown by superimposing the appropriate risk network node symbol on the system node. For the example in Figure 1, the risk network shows an internal and external risk where the probability of occurrence of the internal risk is dependent on the external risk. The system network has three nodes. The direction of dependencies is not shown since it is implied that the overall system network model is representative of a set of layers each with its own dependencies. The network shows that Nodes 1 and 2 are dependent on the external risk and Nodes 1 and 3 are dependent on the internal risk.

Finally, the plot shows the vulnerability of each node over time. By quantifying the vulnerability of each node, these values can be compared to threshold values that allow system analysts to be alerted when a node is either hypervulnerable or approaching hypervulnerability. In the plot shown, the value for Node 1 is above the threshold for hypervulnerability most of the time. This indicates that actions that increase the overall resilience of Node 1 may be best.

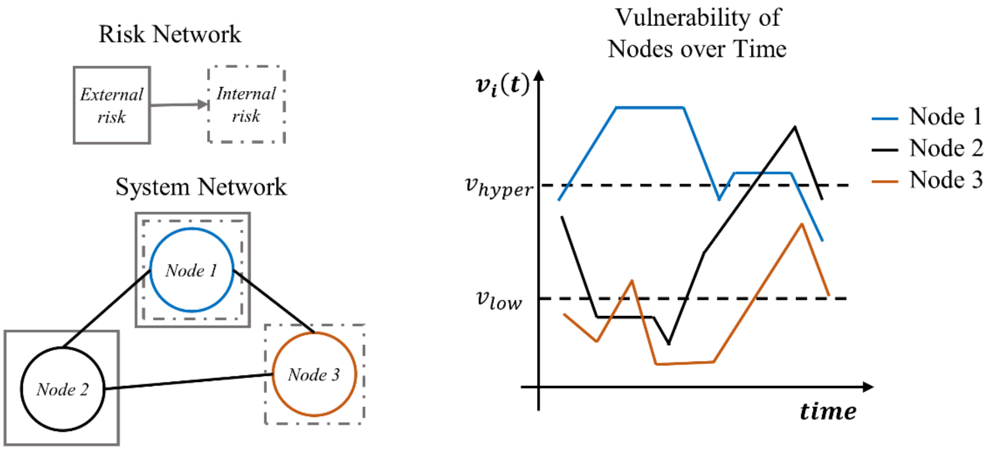


Figure 1. Hypothetical risk and system networks with vulnerability of system nodes compared to threshold values.

4. Results and Discussion

In this section, the layered network dependency methodology previously developed by the authors (Smith et al., 2022; Smith et al., 2021) will be applied to a maritime port in order to allow an analysis and discussion using the definition of hypervulnerability developed in this work.

4.1. Case Study

In this work, the ARNDA methodology will be applied to a maritime port that serves freight with multi-modal transport including ships, rail, and trucks. Since many ports have separate stacks for rail, the port model will be simplified to show only operations involving ships, trucks, and the container stacks dedicated to serving containers traveling by those modes of transport. Figure 2 shows a generalized schematic for a maritime port. Subsequently, Figure 3 shows the resulting risk and system networks similar to the conceptual example from Figure 1.

To apply the layered network dependency methodology, each node needs to have the operability, or performance, of each node must be quantified. It is important to monitor performance of ports using key performance indicators compared to target, or goal, values to close the feedback loop and generate increases in port performance (United Nations, 1976). Performance indicators have evolved significantly since 1976 when they were divided into only financial and operational considerations.

More recent publications include additional categories for performance measures such as safety, connectivity, and environmental measures of performance (Easley, Katsikides, Kucharek, Shamo, & Tiedeman, 2017). As climate change, technological advancements, and other factors drive changes in operations across a variety of industries, maritime ports will be required to adapt how they conduct and assess their operations. However, access to data sets that support quantification of these performance indicators is confounded by issues including proprietary or secure nature of data (Varma, 2008).

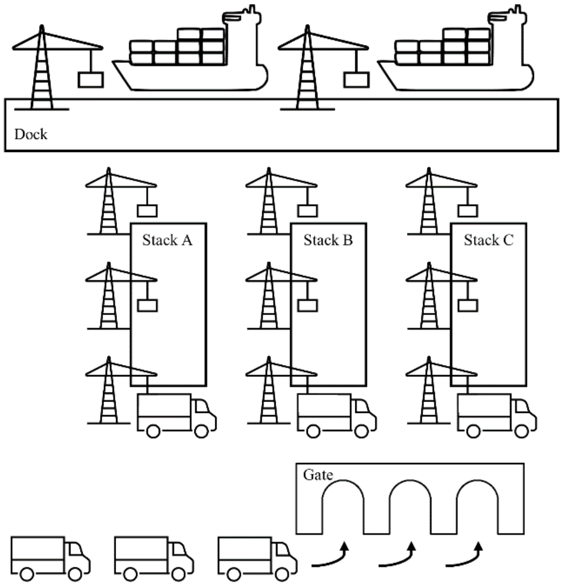


Figure 2. Schematic for a generalized maritime port.

As such, this work will focus on a compromise to time-based measurements which can be estimated from existing small datasets and extended using simulation. The operability of each node will be based on processing or service time at that node.

4.2. Results

The layered network dependency methodology will be applied to the system and risk network shown in Figure 3. The system network has two layers: (1) containers moving towards the stacks, and (2) containers moving away from the stacks.

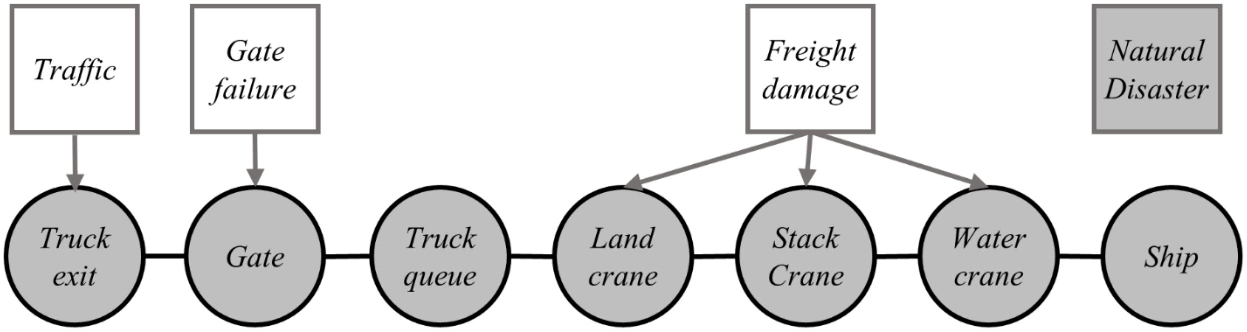
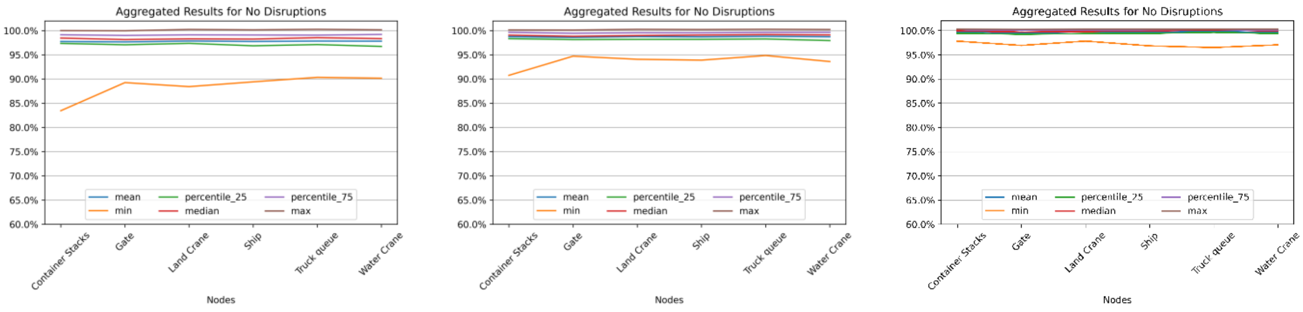


Figure 3. Combined risk (grey square nodes) and system (black circular nodes) networks for the port example.



(a) (b) (c)

Figure 4. Port performance results by node combining network layers using (a) minimum, (b) mean, and (c) maximum aggregation.

The results are shown in Figure 4 for no disruptions meaning that none of the states for the risk network were set to true. That does not mean that the nodes could not enter into a disrupted state (and in fact the results show they likely did), but that there were no external disruptions in this particular case study.

It is important to note that the y-axis in Figure 4 is performance which is inversely related to vulnerability. Therefore, it is expected that the threshold values would be reversed from those in Figure 1. Upon inspecting the results from the analysis, it becomes clear that the container stacks show the widest range in performance under both minimum and mean aggregation. This indicates that under normal operating conditions, the container stacks are indicating that they are hypervulnerable compared with the other nodes.

5. Conclusions

This paper provided background on vulnerability theory and subsequently developed a quantitative definition of vulnerability. This definition was expanded upon to provide initial theory and definition for hypervulnerability and its application to a small hypothetical example. An example application to a maritime port under normal operation was provided supported by an existing framework for port resilience developed by the authors.

While progress has been made towards a quantitative definition of vulnerability that supports the ability to compare nodes within a system and determine which are hypervulnerable, this is still an area that is ripe for further study. First, it would be prudent to extend the port student from Section 4 to include disruptions. Also, there is a need to further explore the connection between various performance metrics and vulnerability.

Funding

This work was funded by the Coastal Virginia Center for Cyber Innovation as "A simulation-based framework for identifying, assessing, and mitigating systemic cybersecurity at the operational technology" under project number 2021ODU-06.005.

References

Blackhurst, J., Craighead, C. W., Elkins, D., & Handfield, R. B. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions. *International Journal of Production Research, 43*(19), 4067-4081.

Brown, B. (2019). Courage and vulnerability part i: Denitions and myths. Retrieved from https://brenebrown.com/wp-content/uploads/2019/08/Integration-Ideas_Courage-and-Vulnerability-Part-1-Definitions-and-Myths.pdf

Burton, C. G. (2015). A validation of metrics for community resilience to natural hazards and disasters using the recovery from Hurricane Katrina as a case study. *Annals of the Association of American Geographers, 105*(1), 67-86.

Calatayud, A., Mangan, J., & Palacin, R. (2017). Vulnerability of international freight flows to shipping network disruptions: A multiplex network perspective. *Transportation Research Part E: Logistics and Transportation Review, 108*, 195-208.

Charrahy, Z., Yaghoobi-Ershadi, M. R., Shirzadi, M. R., Akhavan, A. A., Rassi, Y., Hosseini, S. Z., . . . Hanafi-Bojd, A. A. (2021). Climate change and its effect on the vulnerability to zoonotic cutaneous leishmaniasis in Iran. *Transboundary and emerging diseases.*

Easley, R., Katsikides, N., Kucharek, K., Shamo, D., & Tiedeman, J. (2017). *Freight performance measure primer*. Retrieved from

Garvey, P. R., & Pinto, C. A. (2009). *Introduction to* *functional dependency network analysis.* Paper presented at the The MITRE Corporation and Old Dominion, Second International Symposium on Engineering Systems, MIT, Cambridge, Massachusetts.

Guariniello, C., & DeLaurentis, D. (2017). Supporting design via the system operational dependency analysis methodology. *Research in Engineering Design, 28*(1), 53-69.

Havlin, S., Kenett, D., Bashan, A., Gao, J., & Stanley, H. (2014). Vulnerability of network of networks. *The European Physical Journal Special Topics, 223*(11), 2087-2106.

Leontief, W. (1951). *The Structure of american Economy, 1919-1939: An Empirical Application of Equilibrium Analysis*: Oxford Univ Press.

Li, Y., Chen, K., Collignon, S., & Ivanov, D. (2021). Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability. *European Journal of Operational Research, 291*(3), 1117-1131.

Mustafa, D., Ahmed, S., Saroch, E., & Bell, H. (2011). Pinning down vulnerability: from narratives to numbers. *Disasters, 35*(1), 62-86.

Oxford English Dictionary. (Ed.) (2021) Oxford English Dictionary.

Pandit, P. S., Doyle, M. M., Smart, K. M., Young, C. C., Drape, G. W., & Johnson, C. K. (2018). Predicting wildlife reservoirs and global vulnerability to zoonotic Flaviviruses. *Nature communications, 9*(1), 1-10.

Platto, S., Wang, Y., Zhou, J., & Carafoli, E. (2021). History of the COVID-19 pandemic: Origin, explosion, worldwide spreading. *Biochemical and biophysical research communications, 538*, 14-23.

Ross, R., McEvilley, M., & Oren, J. (2016). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems*. Retrieved from

Smith, K., Diaz, R., & Shen, Y. (2022). Development of a framework to support informed shipbuilding based on supply chain disruptions. *Procedia Computer Science, 200*, 1093-1102.

Smith, K., Diaz, R., Shen, Y., & Longo, F. (2021). *Conceptual development of a probabilistic graphical framework for assessing port resilience*. Paper presented at the 23rd International Conference on Harbor, Maritime and Multimodal Logistics Modeling and Simulation (HMS 2021) Online. https://www.proceedings.com/61129.html

Tate, E. (2012). Social vulnerability indices: a comparative assessment using uncertainty and sensitivity analysis. *Natural Hazards, 63*(2), 325-347.

The Port of Virginia. (2016). *2065 Master Plan*. Retrieved from https://www.portofvirginia.com/wp-content/uploads/2016/02/TPOV-master-plan-2065-final-020316.pdf

Thekdi, S. A., & Santos, J. R. (2016). Supply chain vulnerability analysis using scenario-based input-output modeling: Application to port operations. *Risk Analysis, 36*(5), 1025-1039.

United Nations. (1976). *Port performance indicators*. Retrieved from https://unctad.org/en/PublicationsLibrary/tdbc4d131sup1rev1_en.pdf

United Nations Offce for Disaster Risk Reduction. (2021). Vulnerability. Retrieved from https : / / www .undrr.org/terminology/vulnerability

Varma, A. (2008). *Measurement Sources for Freight Performance Measures and Indicators*. Retrieved from

Wagner, S. M., & Neshat, N. (2010). Assessing the vulnerability of supply chains using graph theory. *International Journal of Production Economics, 126*(1), 121-129.