Maritime Transportation System Risk and Resilience Evaluation

Utkarsha Shirole

Khoury College of Computer Sciences, Northeastern University, Boston

CY5250: Decision Making in Critical Infrastructure

Professor Themis A. Papageorge

06/12/2023

Table of Content

Literature Review

CIKR Sector Background

Critical infrastructure refers to assets, systems, networks, and functions-physical or virtual-that are so critical to the United States that their incapacity or destruction would have a crippling effect on security, national economic security, public health or safety, or any combination of these issues. Key resources are publicly or privately managed resources that are required for the economy and government to function properly. There are 16 critical infrastructures that are part of a complex, interconnected ecosystem. One of the most important sectors of CIKR is the transportation system sector. The nation's transportation system moves people and things throughout the country and around the world in a timely, safe, and secure manner. It is overseen by DHS and the Department of Transportation and is comprised of seven subsectors: highway and motor carrier, aviation, marine transportation system, mass transit and passenger rail, pipeline systems, freight rail, and postal and shipping.

Maritime Transportation System

The Maritime Transportation System (MTS) in the United States is a complex network of waterways, ports, boats, and related infrastructure that is spread across 95,000 miles (about 152887.68 km) of coastline, 361 ports, over 25,000 miles (about 40233.6 km) of waterways and is vital to the country's economy and national security. It involves both domestic and international marine transportation and many components and activities associated to the movement of goods, persons, and services by water. The MTS is a pillar of the American economy. Every year, it permits the passage of nearly 2 billion tons of cargo, the majority of which is international trade. It gives businesses access to global marketplaces and helps industries including manufacturing, agriculture, and retail. MTS accounts for one-quarter of the US GDP and produces around $5.4 trillion each year [6].

The AMHP aims to lower greenhouse gas emissions, conserve energy, enhance safety, lessen landside infrastructure costs, and minimize travel delays brought on by traffic. America’s economic prosperity and standard of living are greatly impacted by congestion on their surface transportation system.

Over the course of the next 30 years, it is anticipated that the total volume of imports and exports handled by their freight system will more than double. Ports, which handle roughly 70% of America's volume of international trade, will be impacted by this. The Secretary designates United States coastal, inland, and intracoastal waters that are commercially navigable as Marine Highway Routes. This covers non-contiguous U.S. ports as well as connections between U.S. and Canadian ports on the Great Lakes-Saint Lawrence Seaway System.

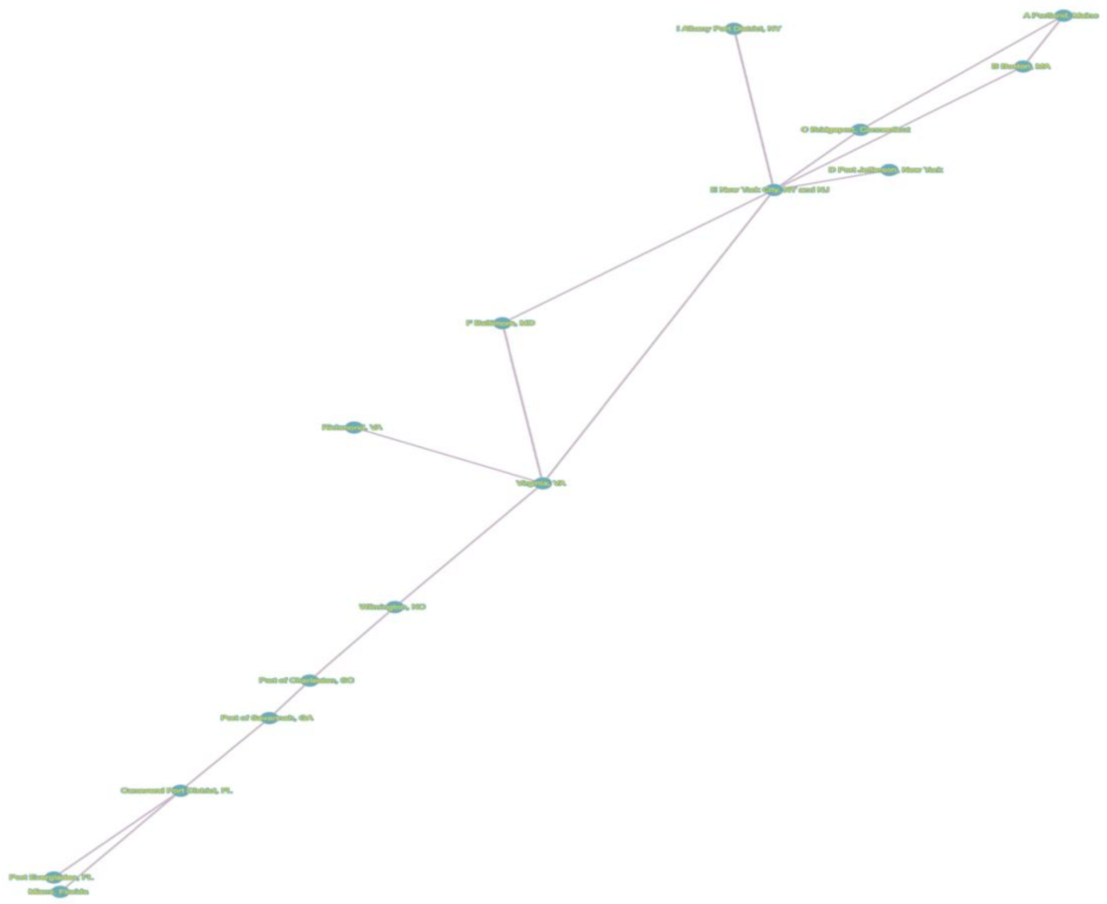
I-95 is the principal North-South landside freight route on the East Coast, The United States Department of Transportation reported more than a dozen severe freight truck bottlenecks along this route, as well as considerable critical rail congestion at the top regions. Future freight traffic projections show increased freight congestion difficulties, with limited opportunity to improve landside capacity.

Mehodology

Network Topology

The M-95 Route contains 15 of the top 50 marine ports in the United States (in terms of overall traffic). These ports handle 582 million short tons of cargo per year, or 26% of the national total. Much of this freight begins or concludes its journey on I-95. Fortunately, the East Coast has a plethora of waterways, bays, rivers, and the Atlantic Ocean. The Route is also flanked by smaller, less congested specialty ports that could play an important role in the expanding marine highway service network. While some Marine Highway operations now serve this Route, there is tremendous room for growth in order to assist address growing congestion, reduce greenhouse gas emissions, conserve energy, and minimize landside infrastructure maintenance costs.

For our paper, we will be considering the M-95 Marine Highway Route and 15 ports that are included in the route as shown in figure [2].



Determining the network graph allows for creating an adjacency matrix based on the links and nodes provided. It is further used to calculate values like node degree, betweenness, and centrality and spectral radius.

Serial No.	Ports	Name	Node Degree
1	Portland, Maine	A	2
2	Boston, MA	B	2
3	Bridgeport, Connecticut	C	2
4	Port Jefferson, New York	D	1
5	New York City, NY and NJ	E	6
6	Baltimore, MD	F	2
7	Virginia, VA	G	4
8	Port Miami, FL	H	1
9	Albany Port District, NY	I	1
10	Richmond, VA	J	1
11	Wilmington, NC	K	2

12	Port of Charleston, SC	L	2
13	Port of Savannah, GA	M	2
14	Canaveral Port District, FL	N	3
15	Port Everglades, FL	O	1

Based on calculations below are the obtained results:

- Degree of the network: 6
- Average node degree: 2.13
- Spectral Radius of the network: 2.913

Vulnerable Nodes

- Further analysis of the adjacency matrix gives us more values:
- Total number of nodes: 15
- Total number of links: 16
- Link Robustness: 6.25%
- Number of links that can be removed: 1
- Node Robustness: 65.68%
- Number of robust nodes: 10
- Number of blocking nodes: 5

Ports	Names	Degree	Node Centrality	Betweenness Centrality	Eigenvector Centrality
New York City, NY and NJ	E	**6**	**0.43**	0.58	**0.60**
Virginia, VA	G	4	0.29	**0.60**	0.44

As per analysis there are 2 vulnerable nodes in the complex network. New York City Port has the highest network degree, node centrality and eigen vector centrality. On the other hand, Virginia Port has the highest betweenness centrality.

It is evident that the adjacency matrix has a spectral radius of 2.913. All nodes together have an average degree of 2.13. A network is deemed complex when its spectral radius is greater than its average node degree.

It is clear there is not much robustness in the link. To break the network, only one link would need to be removed. However, the robustness of the node is relatively high. Before the system breaks, 10 nodes would need to be removed. We were able to estimate the north thanks to the blocking nodes, which prevent the system from being further destroyed. Merely 5 nodes out of 15 would be necessary for the system to continue functioning.

Threat Probabilities

In an era when predators will go to any length to compromise critical infrastructure for illicit objectives, it is advisable to consider that all ports, like nodes in a network, and maritime routes, like links, are vulnerable to persistent threats or the possibility of attacks by malicious actors and adversaries. This assumption assumes that the danger risk for each port (node) and maritime route (link) is around 100%. As a critical component of global trade and connectivity, the marine transportation system requires increased surveillance and strict safety protocols to protect against potential interruptions and hostile activity. As technology advances, guaranteeing the resilience of ports and marine infrastructure becomes increasingly important in fighting the ever-present threat scenario.

Vulnerability Probabilities

The probabilities for each port are calculated with the help of previous attack data and number of attacks stroked in a year. Then the percentage of attacks on a particular port compared to other ports is considered.

Consequences

United States nation’s ports are the lifelines of their economy. Annually, ships move $1.5 trillion in and out of U.S. ports, and ports support more than 13 million jobs. Hence an attack on any US port will result in a huge amount of loss to the government. Since we are not considering any global ports, we only consider the domestic profits. Let's consider that domestic trade provided by the given ports is 5% of the total trade, and since we haven’t considered all the Marine National Highways (there are 31 marine National Highways), the total values estimate to be around $2410 million [8]. By further reducing the $1000 million which is given back as tax to the government for customs and $400 for maintenance of all ports and salaries of people working at the ports, we get a total consequence of $1010 million. Dividing these equally to all the 15 ports allots $70 million for each port and $20 million extra to New York and Virginia ports each as they are responsible for maximum profits and giving some amount lesser to the ports like Port Everglades and Albany port.

Prevention Costs

The budget allocated by President for Port Infrastructure Development Program (PIDP) will be $680 million in 2024 according to award funds to upgrade port infrastructure and amenities, as well as to boost economic growth in and around ports, while also increasing safety, tackling climate change and fairness, and strengthening our supply networks. This includes funding of $450 million which will be provided by the Bipartisan Infrastructure Law (BIL) to support the Port Infrastructure Development Program (PIDP) and will be invested in new grants. The

President's budget asks an extra $230 million to assist PIDP and allow MTS to continue upgrading the ports to help decrease the costs of transferring commodities from ships to shelves and from American farmers and industry to international destinations. Hence, we consider $450 million for all the ports included and $230 million for all the links which will be divided equally among all the links. Since ports like New York, NY & NJ and Virginia, VA have more network degree and are more vulnerable compared to other nodes we slightly assign more 10$ million extra prevention cost to them. On the other hand, ports like Port Miami, FL and Port Everglades, FL are less vulnerable hence we allot 10$ million less prevention cost while keeping all the remaining port prevention costs as 30$ million.

Response Costs

The U.S. Merchant Marine Academy (USMMA)'s FY 2024 budget plan includes $92 million for emergency and recurrent maintenance and repair work on campus, as well as large improvements in aging facilities and infrastructure. As per port centrality and eigenvector centrality value, we have considered a budget of $10 million for each port considering New York port, Virginia port, Wilmington port, $9 million for Canaveral Port District, FL, $4 million for Port Everglades and Port Miami, FL and $5 million each for all the remaining ports.

MBRA Network Analysis

Risk Ranking:

New York City, NY and NJ (Port E):

High Degree (6): Indicates a significant number of connections, potentially making it more susceptible to various attacks.

High Node Centrality (0.43): It suggests that the New York City port is important in terms of the overall network structure.

High Betweenness Centrality (0.58): Indicates that this port plays a critical role in connecting different parts of the network.

High Eigenvector Centrality (0.60): This infers influence and importance within the network.

Virginia, VA (Port G):

Lower Degree (4) compared to Port E, indicating fewer direct connections.

Moderate Node Centrality (0.29): Indicates some importance in the network.

High Betweenness Centrality (0.60): Despite the lower degree, it has high betweenness, suggesting a key role in connecting other nodes.

Moderate Eigenvector Centrality (0.44): Indicates a moderate level of influence.

Vulnerability Ranking:

New York City, NY and NJ (Port E):

High Node Centrality: Higher centrality suggests that if this port is compromised, it may have a cascading effect on the entire network.

High Betweenness Centrality: Being a critical connector, its compromise could disrupt the flow of goods and information.

High Eigenvector Centrality: Its compromise might affect the overall stability and resilience of the network.

Virginia, VA (Port G):

High Betweenness Centrality: Even with a lower degree, its compromise could still have a significant impact on the overall network connectivity.

Moderate Node Centrality: While important, it may not have as critical an impact as Port E.

Moderate Eigenvector Centrality: Indicates a moderate level of influence; compromise may have a noticeable but not overwhelming effect.

Threat Ranking:

New York City, NY and NJ (Port E):

High Degree and Centrality Metrics: Attracts more attention from potential threats due to its significance.

High-profile target due to its central role in the network.

Virginia, VA (Port G):

High Betweenness Centrality: Attracts threats aiming to disrupt network connectivity.

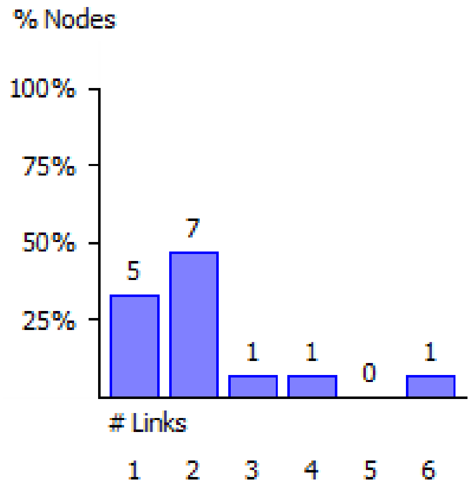
May be targeted for its role as a critical connector.

MBRA Graph

Degree Graph

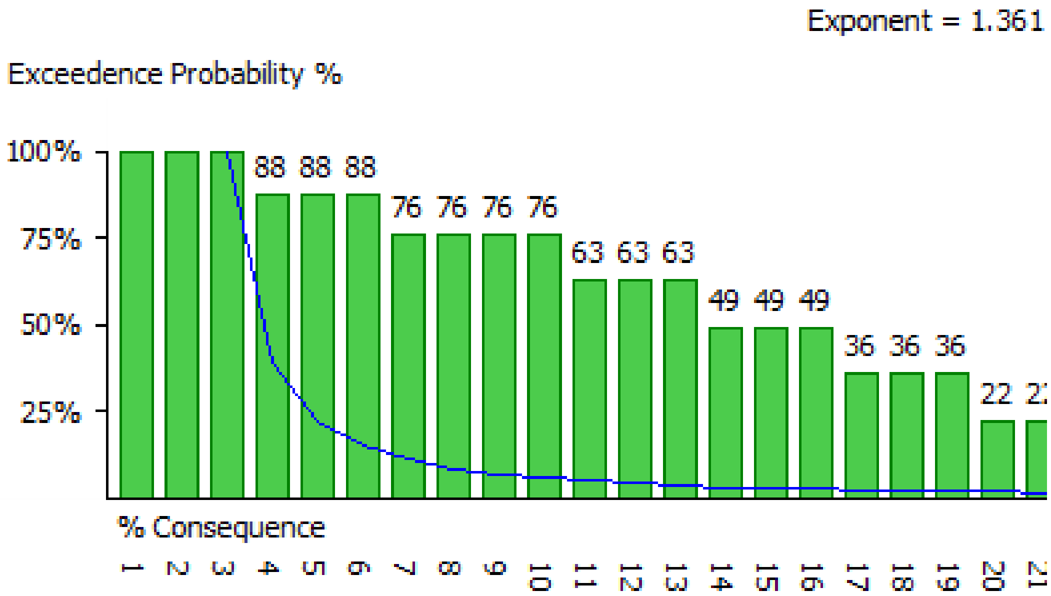
According to the node degree graph, most nodes in the network are connected by a double link. The tail end of the graph with the most links, such as 4 and 6, has a low number of links.

We can observe that the graph follows a logarithmic curve roughly. Most nodes are discovered with two links. This is to be expected because many ports receive freight by a greater capacity port. This statement can be backed by examples like New York Port and Virginia Port with 6 and 4 links respectively. The nodes with one link are also important. The nodes with the highest degree (6) are only one. This is a favorable sign because having many nodes with a high degree may result in self-organized criticality. When we combine this information with the previous knowledge that the spectral radius of the system is bigger than the average degree of the system, we may deduce that another statistic indicates that the maritime port system is less efficient.



Exceedance Probability Graph

The PML Curve for this system has an exponent of 1.361. We know that the risk of PML is high when q is less than one and low when q is larger than one. We remark that a q larger than 1 indicates that the PML risk is minimal in Maritime Transportation (M-95) network. This provides another technique to identify whether the grid is in risk of a cascading failure, as demonstrated by yet another measure.



Resilience Graph

The resilience graph is determined by the resilience to fractal dimension (q), vulnerability of the nodes(V) and the proportionality constant (k) which depends on the type of network and hazard being modeled. The equation derived is as below:

$\text{Log}(q) = b + k * (\text{spectral radius} * V)$

Based on extensive simulation work of Lewis and in reference to [6] the values of b and k are 0.5, -0.42 respectively. As per the above calculations, the spectral Radius of the network is 2.913.

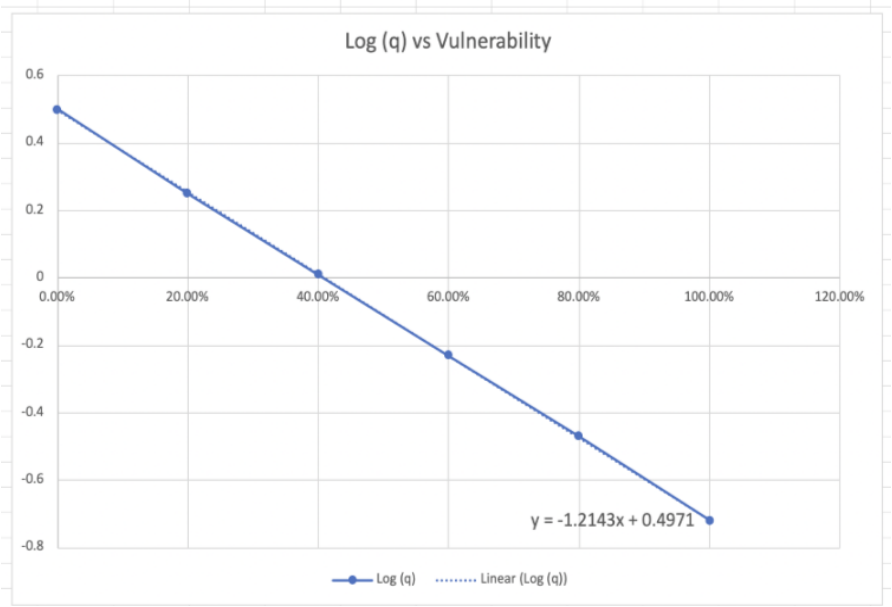
$\text{Log}(q) = 0.5 + (-0.42) * (2.913) * V$

Log (q) = 0.5 + (-1.22) *V

y = -1.2143x + 0.4971

To calculate the critical vulnerability, we see where the graph intersects The Y axis on 0, as log (1) = 0.

Critical Vulnerability is 0.40, that is 40%. This infers that if the vulnerability of the nodes and links exceeds 40% the system is likely to fail.



Fault Tree Analysis

Attacks

As the Maritime Transportation System deals with other countries the probability of attacks is higher compared to other sectors. M-95, being the marine highway route, is in the eastern part of America. This route consists of main ports like Miami, New York and Virginia.

There are two types of attacks possible:

Targeted Attacks: In Targeted attacks, the organization is singled out as the attacker has some intent of disrupting the business or has been paid to do so. A targeted attack is more damaging as it is quite excellently planned to take into consideration the consequences that follow.

Random Attacks: In Random attacks, attackers indiscrimately target as many ports, systems and services as possible. They do not consider the number of machines compromised, the number of users affected and services with vulnerabilities get compromised.

Targeted Attacks on Maritime System:

- State Sponsored attack on Vulnerable Nodes: As per our above results, we consider that nodes like New York and Virginia Port can undergo a cyber-attack and the system can be compromised. Attackers can interrupt operations like imports and exports to domestic and international ports by shutting down the normal working systems. This can cause a lot of damage financially to the government.
- Hijacking the Port: There are pirates and other governments in international waters that can possibly hijack the vulnerable port. Since New York port has the highest network degree it supplies variety of goods to different ports and then the goods are further

transported to other ports. If New York port gets hijacked where the attackers capture the workers and break down the computer systems that are used to communicate and maintain records of import and exports, it will have bad consequences. Many ports have Fishing and recreational boats on hand that terrorists could use to disguise their approach to a target ship.

Random Attacks on Maritime System:

- Port areas and ships in ports are highly vulnerable to terrorist assault. Port regions have particularly broad landside perimeters to safeguard, providing terrorists with numerous possible landside entrance sites. Some ports are placed immediately near to densely populated urban areas, providing terrorists with cover as they approach or flee port districts. Terrorists can utilize a truck to transport themselves and their weapons into a port since large numbers of trucks pass in and out of ports. Attack of any Port will disrupt the smooth operations. For e.g.: A attacker wants financial gain and hence he can randomly choose to attack a port that is easy to conquer.
- Vessel Exploitation: Unscrupulous shipowners have been known to conceal their identities by re-registering their vessels under bogus corporate names, as well as rebranding and repainting their ships. Shipowners can register their vessels under a "flag of convenience" in nations with loose regulations and few requirements for applicants. According to published reports, US intelligence agencies believe they have identified 15 cargo ships with al Qaeda affiliations.

Threats

1. Vessel Exploitation

Vessel exploitation refers to hostile operations directed at marine assets, including ships, tankers, and freight carriers. These operations are intended to jeopardize the integrity, safety, or functionality of marine vessels, posing serious threats to the marine Transportation System (MTS).

Potential Threats:

- Threat actors may attempt to obtain illegal access to vessels, jeopardizing onboard systems and control mechanisms.
- Exploiting weaknesses in navigation systems can result in incorrect positioning information, potentially leading to crashes, groundings, or unauthorized diversions.
- Interference with communication systems: Disrupting onboard communication systems can cut vessels off from traffic management networks, affecting coordination and reaction to navigational issues.
- Cargo Tampering: Threats may include tampering with cargo onboard vessels, which could result in theft, damage, or the introduction of illegal goods into the supply chain.

2. Malware Spread Through Network

Malware proliferation over the network is a cybersecurity problem that involves the entry and transmission of malicious software within the network architecture of the Maritime Transportation System (MTS). This danger has the potential to endanger the confidentiality, integrity, and availability of vital maritime systems.

Potential Threats:

- Ransomware Attack: Malware such as ransomware can encrypt crucial data, causing operational disruptions and potential financial losses.
- Data Exfiltration: Malicious malware may attempt to steal sensitive data from marine networks, such as cargo manifests, operating plans, and navigation data.
- Communication Disruption: Malware can target communication networks, preventing the sharing of essential information between ships, ports, and marine authorities.
- System Degradation: Malware can cause system slowdowns or breakdowns, reducing the efficiency of maritime operations and potentially jeopardizing safety.

3. Attack on Port

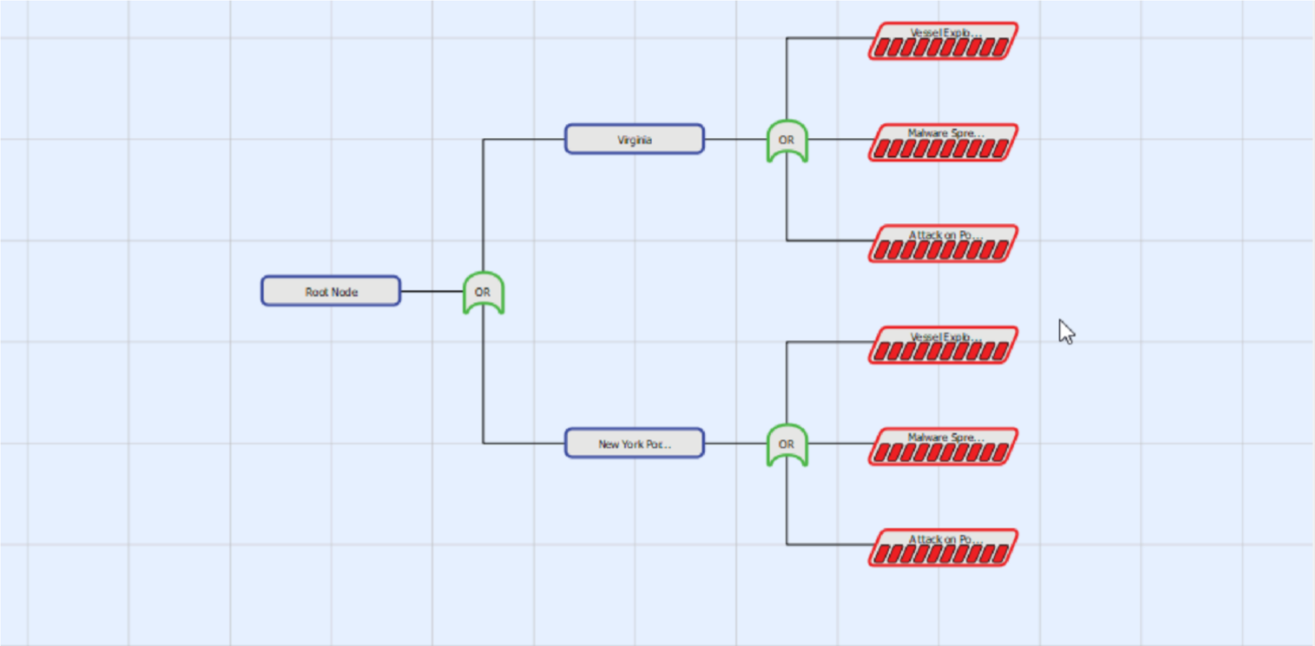
An attack on a port involves purposeful steps to compromise a maritime port's physical and/or digital infrastructure. Such attacks can delay cargo handling, undermine port security, and have a footprint on the entire functionality of the Maritime Transportation System (MTS).

Potential Threats:

- Physical Infrastructure Damage: Port facilities attacks can cause physical damage to docks, cranes, and storage spaces, delaying cargo operations.
- Cyberattacks on Port Systems: Cyber threats may exploit vulnerabilities in port management systems, causing administrative, logistical, and operational functions to be hindered.

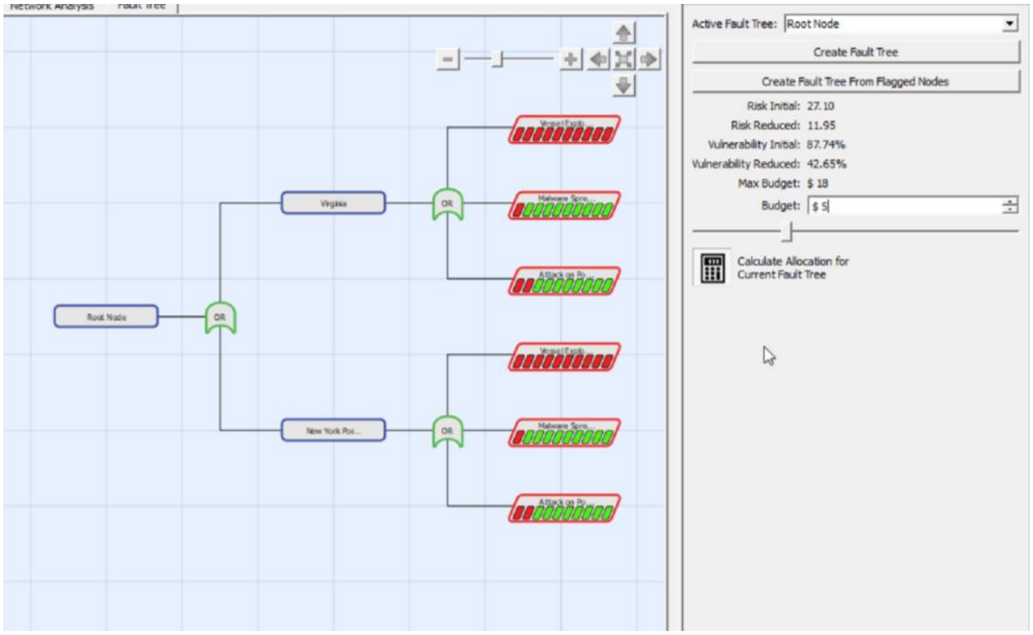
- Disruptions to the Supply Chain: An attack on a port can interrupt the supply chain, causing delays, increased expenses, and severe economic losses.
- Impact on the ecosystem: Some attacks may have environmental consequences, such as oil spills or hazardous substance releases destroying the marine ecosystem.

Fault Tree Analysis



Fault tree analysis helps us to investigate the numerous causes of a particular susceptible node. This study is better suited for nodes with high risk and low resilience. Thus, to demonstrate the range of nodes present, we choose two nodes that are off high risk. Vessel Exploitation, Malware spread through network and attack on the port are the three most prevalent dangers connected with M-95 highway system. The risk for each of these is calculated as a proportion of the total number of such incidents that occur in a decade.

The maximum budget possible for the nodes in $18 million. Applying the budget of $5 million which is 28% approximately the risk is reduced to 11.95 that is by almost 77%. The highest vulnerability reduction takes place in the Malware Spread through Network.



Active Fault Tree: Root Node

Risk Initial: 27.10
Risk Reduced: 11.95
Vulnerability Initial: 87.74%
Vulnerability Reduced: 42.65%
Max Budget: $ 18
Budget: $ 5

Vulnerability Elimination Cost

To eliminate the risks for each individual node, we need to eliminate all the possible threats and vulnerabilities. According to the Fault tree analysis presented above, we can conclude that the vulnerability Elimination cost is $18 million.

Prevention and Response Controls

Mitigating risks in the Maritime Transportation System (MTS), particularly at crucial nodes, entails combining prevention and reaction systems. These policies are designed to improve the cybersecurity posture, physical security, and overall resilience of important nodes like ports and warships. Here are some suggested preventative and reactive measures:

Prevention Controls:

Access Control and Authentication:

Implementing robust access controls and authentication procedures to limit illegal access to vital systems on ships and within ports. To ensure that only authorized personnel may access sensitive systems, use multi-factor authentication, biometric access controls, and role-based access management.

Network Segmentation:

In the case of a cybersecurity incident, using network segmentation to isolate key systems and limiting lateral movement. To contain and mitigate the impact of potential virus distribution, We divide the maritime network into segments, each with its own set of access controls.

Software Updates and Patch Management on a Regular Basis:

Making sure that all software and systems on ships and at ports are kept up to date with the most recent security fixes. Establish a patch management procedure to install security updates as soon as possible, that decrease the risk of exploitation via known vulnerabilities.

Cybersecurity Training:

Conducting frequent cybersecurity training for maritime personnel to raise awareness of potential dangers such as phishing attacks and social engineering. Providing training on detecting and reporting suspicious activity, highlighting the need of cybersecurity hygiene, and cultivating a security-conscious culture.

Physical security measures:

Improving physical security at crucial nodes, such as access points, monitoring, and perimeter controls. To dissuade unwanted access and guard against physical threats, deploy security cameras, fencing, access control points, and security staff.

Response Controls:

Plans for Incident Response:

Creating and testing thorough incident response strategies on a regular basis to enable a quick and effective reaction to cybersecurity issues or physical security breaches. Establishing explicit communication procedures, assigning roles and duties, and conducting tabletop exercises to model response scenarios during implementation.

Forensic Analysis Capabilities:

Building forensic analysis capabilities to analyze and comprehend the nature and consequences of cybersecurity incidents. Implementations include training staff in digital forensics, deploying forensic analysis tools, and forming alliances with outside experts for advanced forensic investigations.

Backup and Recovery methods:

In the case of a ransomware attack or data loss, implementing comprehensive backup and recovery methods to minimize downtime. Backing up vital data on a regular basis, keeping backups in secure locations, and verifying the restoration procedure to assure data integrity.

Plans for Crisis Communication:

Preparing crisis communication strategy to ensure clear and effective communication with stakeholders during security situations. Establishing communication channels, appointing spokespersons, and providing regular updates to the public, employees, and appropriate authorities.

The New York Port, as a critical node, is vulnerable to vessel exploitation. This could include unauthorized entry to vessels, navigation system manipulation, or other harmful operations aimed against maritime assets. Because of its large network infrastructure, the port is vulnerable to virus proliferation. An attack on the network might jeopardize communication systems, data integrity, and key port operations. Given its importance, an attack on the port infrastructure might have far-reaching implications. Physical damage to facilities, disruption of cargo handling operations, or interference with port management systems are all possibilities.

Virginia Port, albeit having a little lesser degree than New York Port, is nevertheless vital and prone to vessel exploitation. Potential risks to maritime navigation and control systems should be addressed by security measures. Virginia Port's network architecture is prone to malware proliferation. To avoid and limit the impact of network-based attacks on port operations, adequate cybersecurity measures are required. With its high betweenness centrality, Virginia Port could be a target for direct strikes. Security protocols should prioritize preventing and responding to physical and cyber threats to the port's infrastructure.

Role of National Cybersecurity Entities and Workforce Recommendation

Coordination and Information Sharing: National cybersecurity agencies play an important role in coordinating cybersecurity efforts across multiple sectors, including marine transportation.

They improve situational awareness by facilitating information exchange across government agencies, private sector players, and foreign partners.

Incident Response and Threat Intelligence: These organizations are in charge of establishing and implementing incident response strategies to combat cyber threats as soon as possible.

They collect and evaluate threat intelligence in order to better understand the developing cyber threats and vulnerabilities in the marine environment.

Regulation and Standards: National bodies may implement maritime-specific cybersecurity regulations and standards to ensure that enterprises comply to best practices and minimal security requirements.

Capacity Building: They may participate in capacity-building activities, such as training and resource distribution, to improve the cybersecurity posture.

Specific Training: Create and implement specific cybersecurity training programs suited to the marine industry's particular concerns. This covers incident response, risk management, and secure coding techniques training.

Collaboration with Educational Institutions: Encourage collaboration among government agencies, industry stakeholders, and educational institutions in order to develop academic programs that generate qualified cybersecurity experts with an emphasis on maritime cybersecurity.

Qualifications and certifications: Encourage cybersecurity specialists working in the marine sector to get industry-recognized certifications to assure a baseline level of proficiency.

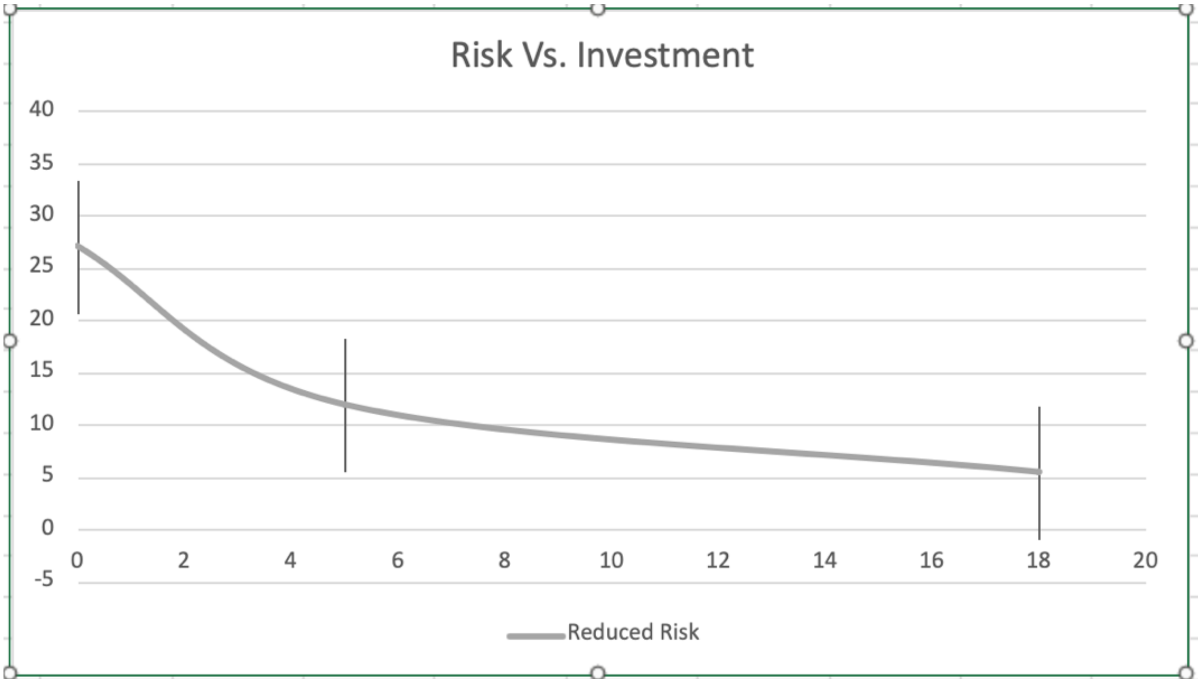
Strategies for Recruitment and Retention: Implement measures such as competitive salary, professional growth opportunities, and a supportive work environment to recruit and retain cybersecurity talent in the marine industry.

Public-Private Partnerships: Facilitate collaboration between government and private groups in order to exchange knowledge, resources, and information.

Return on Investment (ROI) Consideration

Return of Investment

After analysing the Fault Tree analysis, we get values for initial risk and reduced risk and the investments done for them to be reduced. On plotting the Risk Vs Investment Graph it is clear that in the investment should be done around $5 million dollars. More than $5 million investment will not result in any more reduction of risk.



Funding Resources:

The FAST Act is a federal statute that guarantees long-term funding for surface transportation infrastructure planning and investment.

The FAST Act contains several programs that may be applicable to marine highway projects, including INFRA (Infrastructure for Rebuilding America), CMAQ (Congestion Mitigation and

Air Quality Program), STBG (Surface Transportation Block Grant Program), and NHFP (National Highway Freight Program).

The NHFP supports numerous objectives, including the following for marine highway projects:

- Investing in infrastructure and operational improvements that boost economic competitiveness, reduce congestion, lower freight transportation costs, improve reliability, and boost productivity.
- Improving the NHFN's (National Highway Freight Network) efficiency and productivity
- Improving state flexibility to support multi-state corridor planning and address highway freight connectivity.
- NHFP funding contributes to the efficient movement of freight on the NHFN and should be identified in the state's freight investment strategy.

Conclusion

A thorough examination of the M-95 Highway within the context of the Maritime Transportation System reveals a complicated network with deep interactions between nodes and linkages. Critical vulnerabilities and hazards have been discovered using sophisticated approaches such as MBRA and complex network analysis, laying the groundwork for strategic risk reduction and resilience enhancement activities. The resilience and susceptibility of the M-95 network were assessed using a variety of metrics, including node degrees, network degrees, link robustness, spectral radius, node robustness, and centrality measurements. The results of the Random Attacks and Targeted Attacks simulations revealed possible vulnerabilities and crucial nodes, emphasizing the importance of a proactive cybersecurity approach.

MBRA integration aided in the calculation of risks, critical nodes, and the development of the Resilience equation, resulting in a better knowledge of the system's weaknesses. Proposed preventative and reaction controls were examined, with an emphasis on reinforcing Critical Nodes, especially those with high betweenness centrality.

Fault Tree Analysis (FTA) for key nodes introduced another level of complexity to the risk assessment, providing Vulnerability Elimination Costs and appropriate budget allocations. Recommendations for risk mitigation and resilience enhancement were made, highlighting the need of having a well-defined budget that is linked with strategic aims.

In summary, protecting the M-95 Highway necessitates a holistic strategy that incorporates technology improvements, rigorous risk management systems, and stakeholder participation. As the marine sector evolves, a strong M-95 Highway not only assures the safe movement of products but also helps to overall economic stability and national security.

References

[1] https://www.cyber.nj.gov/threat-analysis-reports/maritime-threat-analysis

[2] https://www.transportation.gov/testimony/short-sea-shipping-rebuilding-america%E2%80%99s-maritime-industry#_ftnref4

[3] https://www.everycrsreport.com/reports/RL31733.html

[4] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5634440

[5] https://www.maritime.dot.gov/sites/marad.dot.gov/files/2020-10/PPIT%20Marine%20Highway%20Module%20Final%20200831_ADA_wappendices.pdf

[6] https://www.jstor.org/stable/26846119?seq=4

[7] https://www.transportation.gov/fiscal-year-2024-budget-and-implementation-ocean-shipping-reform-act

[8] https://coast.noaa.gov/states/fast-facts/ports.html

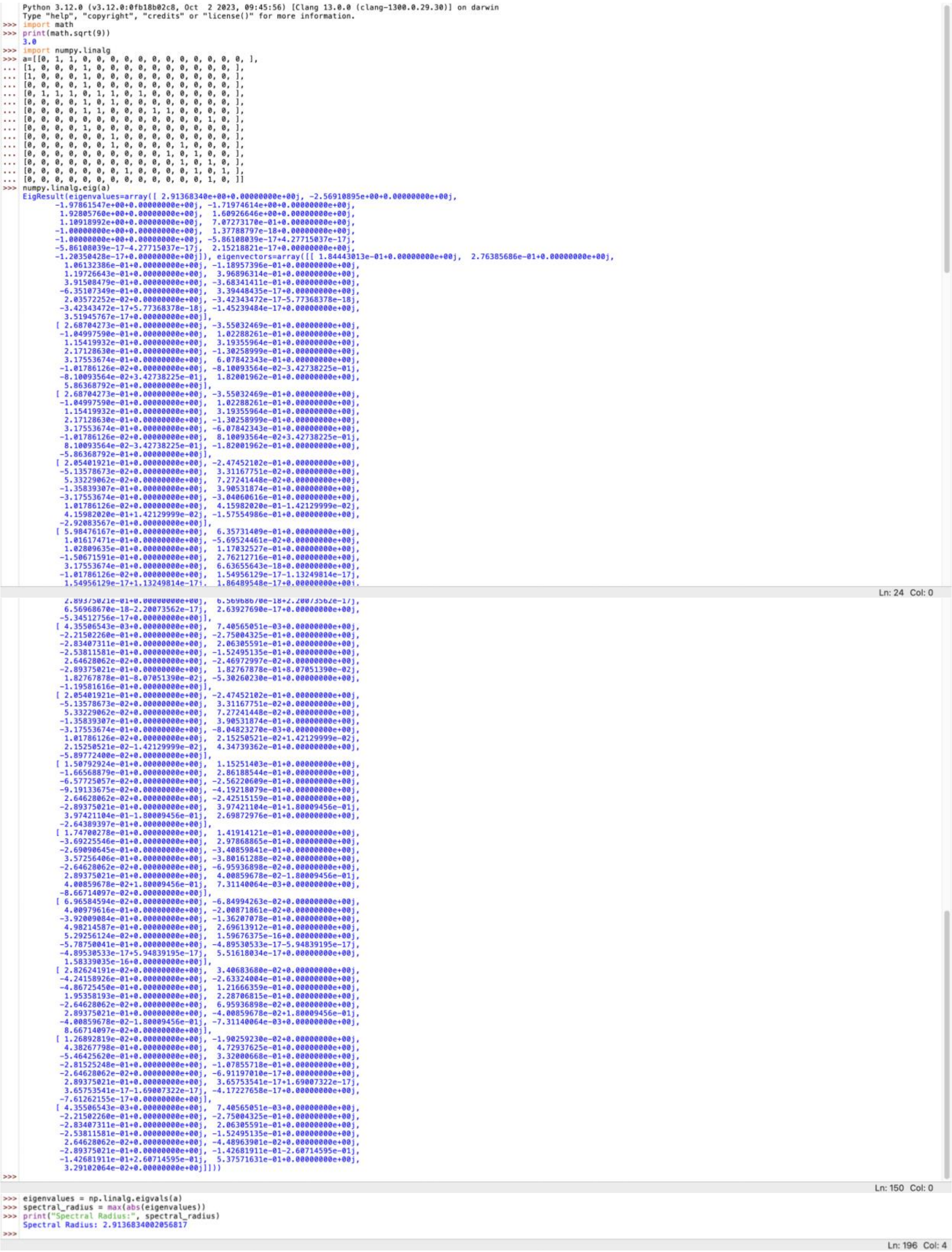
Graph reference:
[1] https://maps.dot.gov/portal/apps/dashboards/ca71b716d07449e9b00a8381f9585629

Appendix

Ports vary in size, commodities and cargo types handled, and organizational structure. Facility and operational considerations at a hub container port will be considerably different than at a small general cargo port. Assess each port's current physical assets and operational capabilities with respect to the proposed potential project.

Existing capacity, work rules, types of vessels, highway and rail connectivity, and interaction with other port operations should be considered. Emphasis can be placed on each port's availability of suitable physical sites and facilities and the nature and extent of improvements necessary for a marine highway service to capture potential demand.

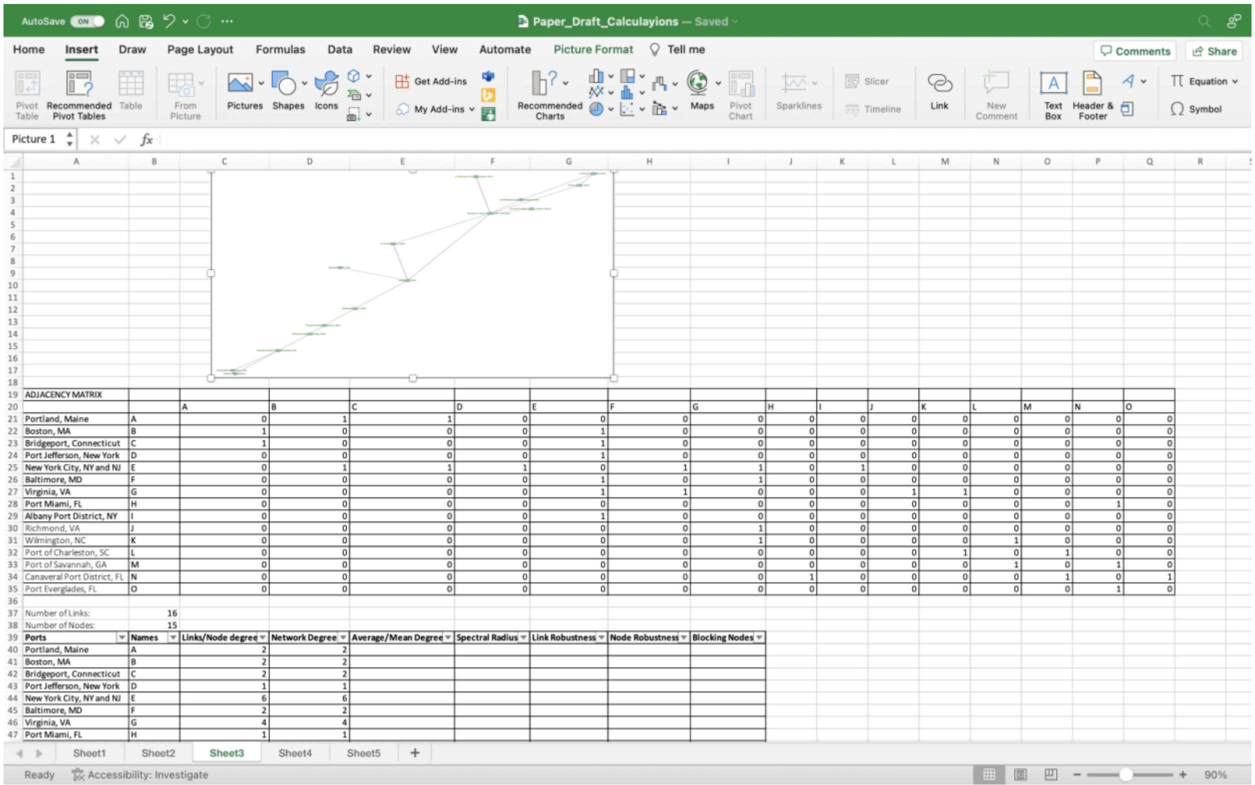
Potential demand is the basic determinant of whether marine highway services can succeed. Potential demand can include collective goods flows such as international containerized cargo moved through major international ports that could be transported relatively long distances to and from coastal areas via water rather than by truck. But demand for marine highway services can also include very commodity-specific and/or more regional niche markets with unique origins and destinations. Successful marine highway development may depend on combining various niche markets that may not be able to stand alone into services that are viable when put together.



```
    Python 3.12.0 (v3.12.0:0fb18b02c8, Oct  2 2023, 09:45:56) [Clang 13.0.0 (clang-1300.0.29.30)] on darwin
    Type "help", "copyright", "credits" or "license()" for more information.
>>> import math
>>> print(math.sqrt(9))
    3.0
>>> import numpy.linalg
>>> a=[[0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ],
... [1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ],
... [1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ],
... [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ],
... [0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, ],
... [0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, ],
... [0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, ],
... [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, ],
... [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ],
... [0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, ],
... [0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, ],
... [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, ],
... [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, ],
... [0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, ],
... [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, ]]
>>> numpy.linalg.eig(a)
    EigResult(eigenvalues=array([ 2.91368340e+00+0.00000000e+00j, -2.56910895e+00+0.00000000e+00j,
            -1.97861547e+00+0.00000000e+00j, -1.71974614e+00+0.00000000e+00j,
             1.92805760e+00+0.00000000e+00j,  1.60926646e+00+0.00000000e+00j,
             1.10918992e+00+0.00000000e+00j,  7.07273170e-01+0.00000000e+00j,
            -1.00000000e+00+0.00000000e+00j,  1.37788797e-18+0.00000000e+00j,
            -1.00000000e+00+0.00000000e+00j, -5.86108039e-17+4.27715037e-17j,
            -5.86108039e-17-4.27715037e-17j,  2.15218821e-17+0.00000000e+00j,
            -1.20350428e-17+0.00000000e+00j]), eigenvectors=array([[ 1.84443013e-01+0.00000000e+00j,  2.76385686e-01+0.00000000e+00j,
               1.06132386e-01+0.00000000e+00j, -1.18957396e-01+0.00000000e+00j,
               1.19726643e-01+0.00000000e+00j,  3.96896314e-01+0.00000000e+00j,
               3.91508479e-01+0.00000000e+00j, -3.68341411e-01+0.00000000e+00j,
              -6.35107349e-01+0.00000000e+00j,  3.39448435e-17+0.00000000e+00j,
               2.03572252e-02+0.00000000e+00j, -3.42343472e-17-5.77368378e-18j,
              -3.42343472e-17+5.77368378e-18j, -1.45239484e-17+0.00000000e+00j,
               3.51945767e-17+0.00000000e+00j],
             [ 2.68704273e-01+0.00000000e+00j, -3.55032469e-01+0.00000000e+00j,
              -1.04997590e-01+0.00000000e+00j,  1.02288261e-01+0.00000000e+00j,
               1.15419932e-01+0.00000000e+00j,  3.19355964e-01+0.00000000e+00j,
               2.17128630e-01+0.00000000e+00j, -1.30258999e-01+0.00000000e+00j,
               3.17553674e-01+0.00000000e+00j,  6.07842343e-01+0.00000000e+00j,
              -1.01786126e-02+0.00000000e+00j, -8.10093564e-02-3.42738225e-01j,
              -8.10093564e-02+3.42738225e-01j,  1.82001962e-01+0.00000000e+00j,
               5.86368792e-01+0.00000000e+00j],
             [ 2.68704273e-01+0.00000000e+00j, -3.55032469e-01+0.00000000e+00j,
              -1.04997590e-01+0.00000000e+00j,  1.02288261e-01+0.00000000e+00j,
               1.15419932e-01+0.00000000e+00j,  3.19355964e-01+0.00000000e+00j,
               2.17128630e-01+0.00000000e+00j, -1.30258999e-01+0.00000000e+00j,
               3.17553674e-01+0.00000000e+00j, -6.07842343e-01+0.00000000e+00j,
              -1.01786126e-02+0.00000000e+00j,  8.10093564e-02+3.42738225e-01j,
               8.10093564e-02-3.42738225e-01j, -1.82001962e-01+0.00000000e+00j,
              -5.86368792e-01+0.00000000e+00j],
             [ 2.05401921e-01+0.00000000e+00j, -2.47452102e-01+0.00000000e+00j,
              -5.13578673e-02+0.00000000e+00j,  3.31167751e-02+0.00000000e+00j,
               5.33229062e-02+0.00000000e+00j,  7.27241448e-02+0.00000000e+00j,
              -1.35839307e-01+0.00000000e+00j,  3.90531874e-01+0.00000000e+00j,
              -3.17553674e-01+0.00000000e+00j, -3.04060616e-01+0.00000000e+00j,
               1.01786126e-02+0.00000000e+00j,  4.15982020e-01-1.42129999e-02j,
               4.15982020e-01+1.42129999e-02j, -1.57554986e-01+0.00000000e+00j,
              -2.92083567e-01+0.00000000e+00j],
             [ 5.98476167e-01+0.00000000e+00j,  6.35731409e-01+0.00000000e+00j,
               1.01617471e-01+0.00000000e+00j, -5.69524461e-02+0.00000000e+00j,
               1.02809635e-01+0.00000000e+00j,  1.17032527e-01+0.00000000e+00j,
              -1.50671591e-01+0.00000000e+00j,  2.76212716e-01+0.00000000e+00j,
               3.17553674e-01+0.00000000e+00j,  6.63655643e-18+0.00000000e+00j,
              -1.01786126e-02+0.00000000e+00j,  1.54956129e-17-1.13249814e-17j,
               1.54956129e-17+1.13249814e-17j,  1.86489548e-17+0.00000000e+00j,
```

```
               2.89375021e-01+0.00000000e+00j,  6.56968670e-18+2.20073562e-17j,
               6.56968670e-18-2.20073562e-17j,  2.63927690e-17+0.00000000e+00j,
              -5.34512756e-17+0.00000000e+00j],
             [ 4.35506543e-03+0.00000000e+00j,  7.40565051e-03+0.00000000e+00j,
              -2.21502260e-01+0.00000000e+00j, -2.75004325e-01+0.00000000e+00j,
              -2.83407311e-01+0.00000000e+00j,  2.06305591e-01+0.00000000e+00j,
              -2.53811581e-01+0.00000000e+00j, -1.52495135e-01+0.00000000e+00j,
               2.64628062e-02+0.00000000e+00j, -2.46972997e-02+0.00000000e+00j,
              -2.89375021e-01+0.00000000e+00j,  1.82767878e-01+8.07051390e-02j,
               1.82767878e-01-8.07051390e-02j, -5.30260230e-01+0.00000000e+00j,
              -1.19581616e-01+0.00000000e+00j],
             [ 2.05401921e-01+0.00000000e+00j, -2.47452102e-01+0.00000000e+00j,
              -5.13578673e-02+0.00000000e+00j,  3.31167751e-02+0.00000000e+00j,
               5.33229062e-02+0.00000000e+00j,  7.27241448e-02+0.00000000e+00j,
              -1.35839307e-01+0.00000000e+00j,  3.90531874e-01+0.00000000e+00j,
              -3.17553674e-01+0.00000000e+00j, -8.04823270e-03+0.00000000e+00j,
               1.01786126e-02+0.00000000e+00j,  2.15250521e-02+1.42129999e-02j,
               2.15250521e-02-1.42129999e-02j,  4.34739362e-01+0.00000000e+00j,
              -5.89772400e-02+0.00000000e+00j],
             [ 1.50792924e-01+0.00000000e+00j,  1.15251403e-01+0.00000000e+00j,
              -1.66568879e-01+0.00000000e+00j,  2.86188544e-01+0.00000000e+00j,
              -6.57725057e-02+0.00000000e+00j, -2.56220609e-01+0.00000000e+00j,
              -9.19133675e-02+0.00000000e+00j, -4.19218079e-01+0.00000000e+00j,
               2.64628062e-02+0.00000000e+00j, -2.42515159e-01+0.00000000e+00j,
              -2.89375021e-01+0.00000000e+00j,  3.97421104e-01+1.80009456e-01j,
               3.97421104e-01-1.80009456e-01j,  2.69872976e-01+0.00000000e+00j,
              -2.64389397e-01+0.00000000e+00j],
             [ 1.74700278e-01+0.00000000e+00j,  1.41914121e-01+0.00000000e+00j,
              -3.69225546e-01+0.00000000e+00j,  2.97868865e-01+0.00000000e+00j,
              -2.69090645e-01+0.00000000e+00j, -3.40859841e-01+0.00000000e+00j,
               3.57256406e-01+0.00000000e+00j, -3.80161288e-02+0.00000000e+00j,
              -2.64628062e-02+0.00000000e+00j, -6.95936898e-02+0.00000000e+00j,
               2.89375021e-01+0.00000000e+00j,  4.00859678e-02-1.80009456e-01j,
               4.00859678e-02+1.80009456e-01j,  7.31140064e-03+0.00000000e+00j,
              -8.66714097e-02+0.00000000e+00j],
             [ 6.96584594e-02+0.00000000e+00j, -6.84994263e-02+0.00000000e+00j,
               4.00979616e-01+0.00000000e+00j, -2.00871861e-02+0.00000000e+00j,
              -3.92009084e-01+0.00000000e+00j, -1.36207078e-01+0.00000000e+00j,
               4.98214587e-01+0.00000000e+00j,  2.69613912e-01+0.00000000e+00j,
               5.29256124e-02+0.00000000e+00j,  1.59676375e-16+0.00000000e+00j,
              -5.78750041e-01+0.00000000e+00j, -4.89530533e-17-5.94839195e-17j,
              -4.89530533e-17+5.94839195e-17j,  5.51618034e-17+0.00000000e+00j,
               1.58339035e-16+0.00000000e+00j],
             [ 2.82624191e-02+0.00000000e+00j,  3.40683680e-02+0.00000000e+00j,
              -4.24158926e-01+0.00000000e+00j, -2.63324004e-01+0.00000000e+00j,
              -4.86725450e-01+0.00000000e+00j,  1.21666359e-01+0.00000000e+00j,
               1.95358193e-01+0.00000000e+00j,  2.28706815e-01+0.00000000e+00j,
              -2.64628062e-02+0.00000000e+00j,  6.95936898e-02+0.00000000e+00j,
               2.89375021e-01+0.00000000e+00j, -4.00859678e-02+1.80009456e-01j,
              -4.00859678e-02-1.80009456e-01j, -7.31140064e-03+0.00000000e+00j,
               8.66714097e-02+0.00000000e+00j],
             [ 1.26892819e-02+0.00000000e+00j, -1.90259230e-02+0.00000000e+00j,
               4.38267798e-01+0.00000000e+00j,  4.72937625e-01+0.00000000e+00j,
              -5.46425620e-01+0.00000000e+00j,  3.32000668e-01+0.00000000e+00j,
              -2.81525248e-01+0.00000000e+00j, -1.07855718e-01+0.00000000e+00j,
              -2.64628062e-02+0.00000000e+00j, -6.91197010e-17+0.00000000e+00j,
               2.89375021e-01+0.00000000e+00j,  3.65753541e-17+1.69007322e-17j,
               3.65753541e-17-1.69007322e-17j, -4.17227658e-17+0.00000000e+00j,
              -7.61262155e-17+0.00000000e+00j],
             [ 4.35506543e-03+0.00000000e+00j,  7.40565051e-03+0.00000000e+00j,
              -2.21502260e-01+0.00000000e+00j, -2.75004325e-01+0.00000000e+00j,
              -2.83407311e-01+0.00000000e+00j,  2.06305591e-01+0.00000000e+00j,
              -2.53811581e-01+0.00000000e+00j, -1.52495135e-01+0.00000000e+00j,
               2.64628062e-02+0.00000000e+00j, -4.48963901e-02+0.00000000e+00j,
              -2.89375021e-01+0.00000000e+00j, -1.42681911e-01-2.60714595e-01j,
              -1.42681911e-01+2.60714595e-01j,  5.37571631e-01+0.00000000e+00j,
               3.29102064e-02+0.00000000e+00j]]))
>>>
```

```
>>> eigenvalues = np.linalg.eigvals(a)
>>> spectral_radius = max(abs(eigenvalues))
>>> print("Spectral Radius:", spectral_radius)
    Spectral Radius: 2.9136834002056817
>>>
```

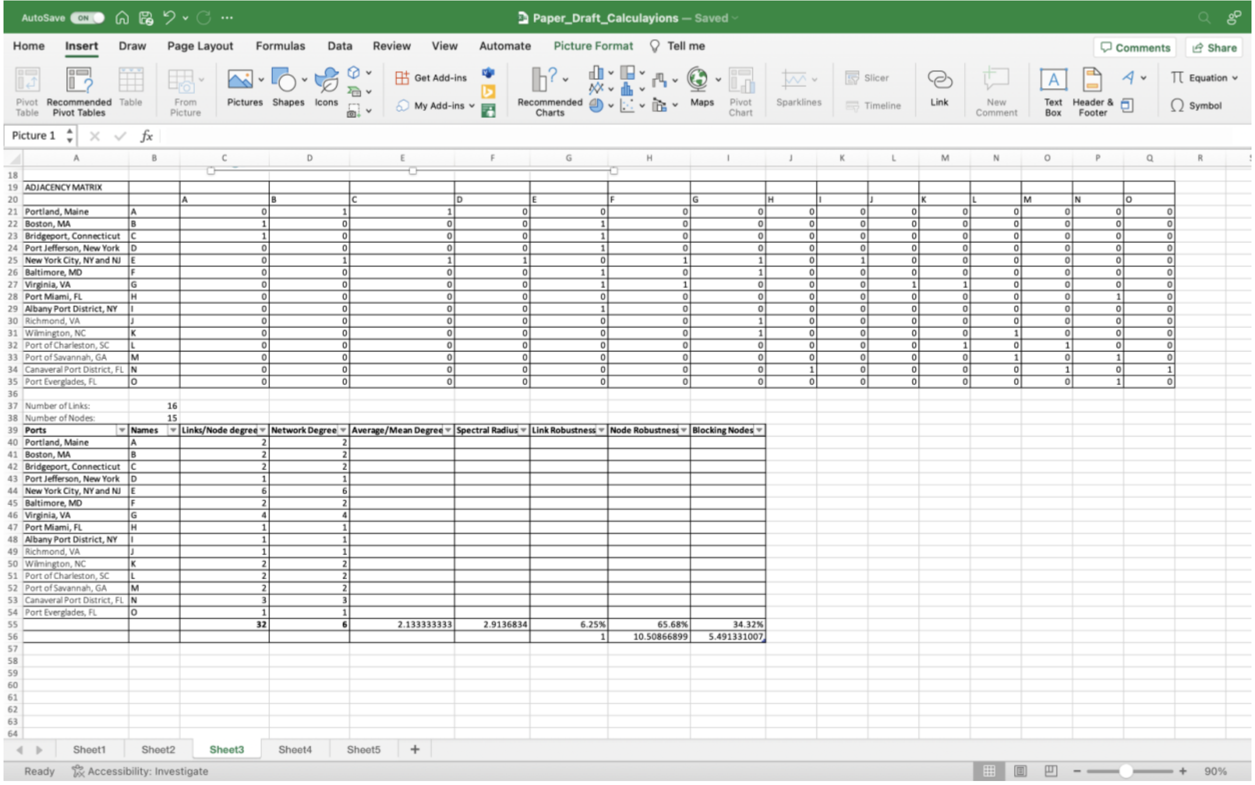


ADJACENCY MATRIX

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Portland, Maine	A	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Boston, MA	B	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Bridgeport, Connecticut	C	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Port Jefferson, New York	D	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
New York City, NY and NJ	E	0	1	1	1	0	1	1	0	1	0	0	0	0	0	0
Baltimore, MD	F	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
Virginia, VA	G	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0
Port Miami, FL	H	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Albany Port District, NY	I	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Richmond, VA	J	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Wilmington, NC	K	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0
Port of Charleston, SC	L	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
Port of Savannah, GA	M	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
Canaveral Port District, FL	N	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1
Port Everglades, FL	O	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Number of Links: 16
Number of Nodes: 15

Ports	Names	Links/Node degree	Network Degree	Average/Mean Degree	Spectral Radius	Link Robustness	Node Robustness	Blocking Nodes
Portland, Maine	A	2	2					
Boston, MA	B	2	2					
Bridgeport, Connecticut	C	2	2					
Port Jefferson, New York	D	1	1					
New York City, NY and NJ	E	6	6					
Baltimore, MD	F	2	2					
Virginia, VA	G	4	4					
Port Miami, FL	H	1	1					



ADJACENCY MATRIX

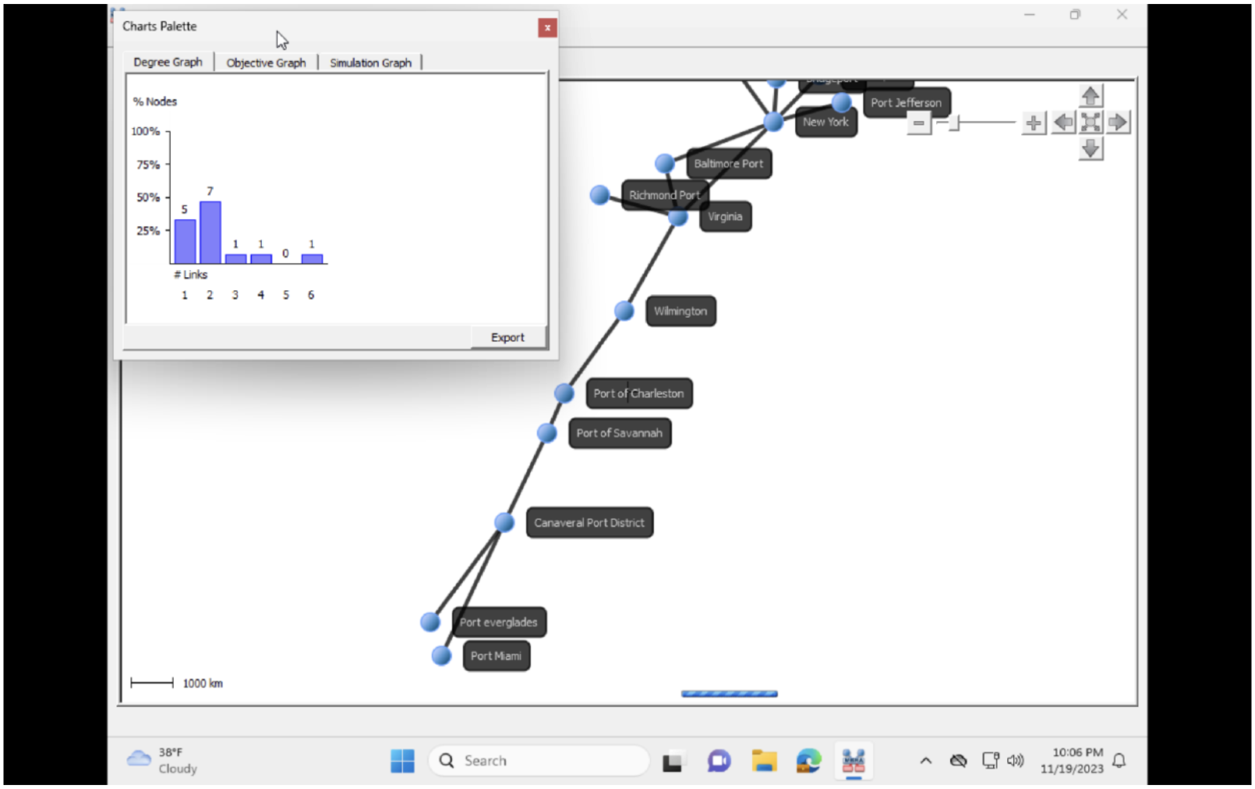
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Portland, Maine	A	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Boston, MA	B	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Bridgeport, Connecticut	C	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Port Jefferson, New York	D	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
New York City, NY and NJ	E	0	1	1	1	0	1	1	0	1	0	0	0	0	0	0
Baltimore, MD	F	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
Virginia, VA	G	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0
Port Miami, FL	H	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Albany Port District, NY	I	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Richmond, VA	J	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Wilmington, NC	K	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0
Port of Charleston, SC	L	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
Port of Savannah, GA	M	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
Canaveral Port District, FL	N	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1
Port Everglades, FL	O	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

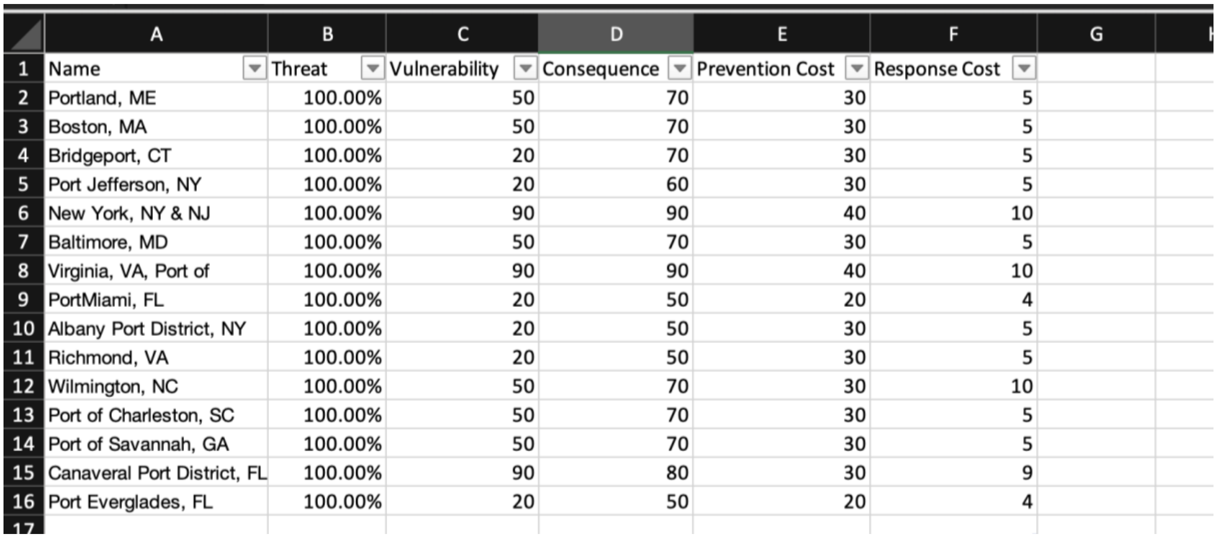
Number of Links: 16
Number of Nodes: 15

Ports	Names	Links/Node degree	Network Degree	Average/Mean Degree	Spectral Radius	Link Robustness	Node Robustness	Blocking Nodes
Portland, Maine	A	2	2					
Boston, MA	B	2	2					
Bridgeport, Connecticut	C	2	2					
Port Jefferson, New York	D	1	1					
New York City, NY and NJ	E	6	6					
Baltimore, MD	F	2	2					
Virginia, VA	G	4	4					
Port Miami, FL	H	1	1					
Albany Port District, NY	I	1	1					
Richmond, VA	J	1	1					
Wilmington, NC	K	2	2					
Port of Charleston, SC	L	2	2					
Port of Savannah, GA	M	2	2					
Canaveral Port District, FL	N	3	3					
Port Everglades, FL	O	1	1					
		32	6	2.133333333	2.9136834	6.25%	65.68%	34.32%
						1	10.50866899	5.491331007

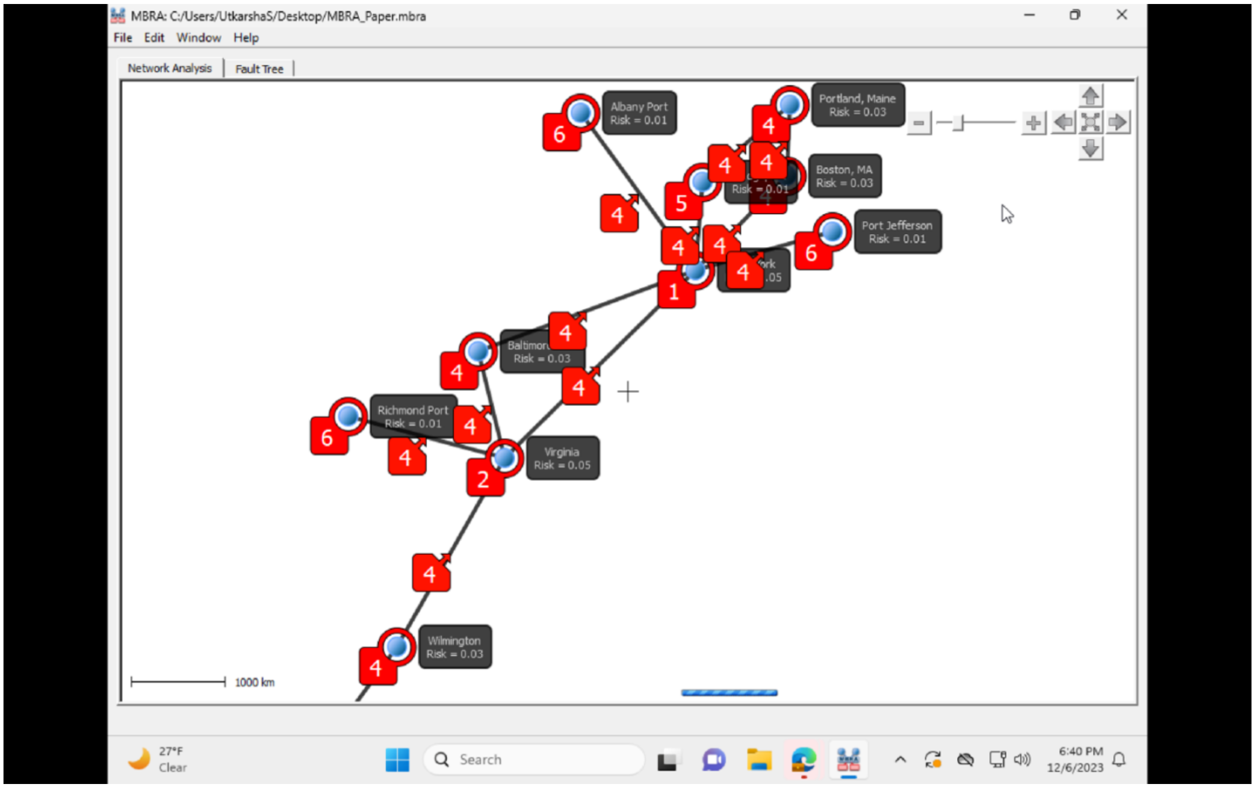
Ports	Names	Degree	Node Centrality	Betweenness Centrality	Eigenvector Centrality

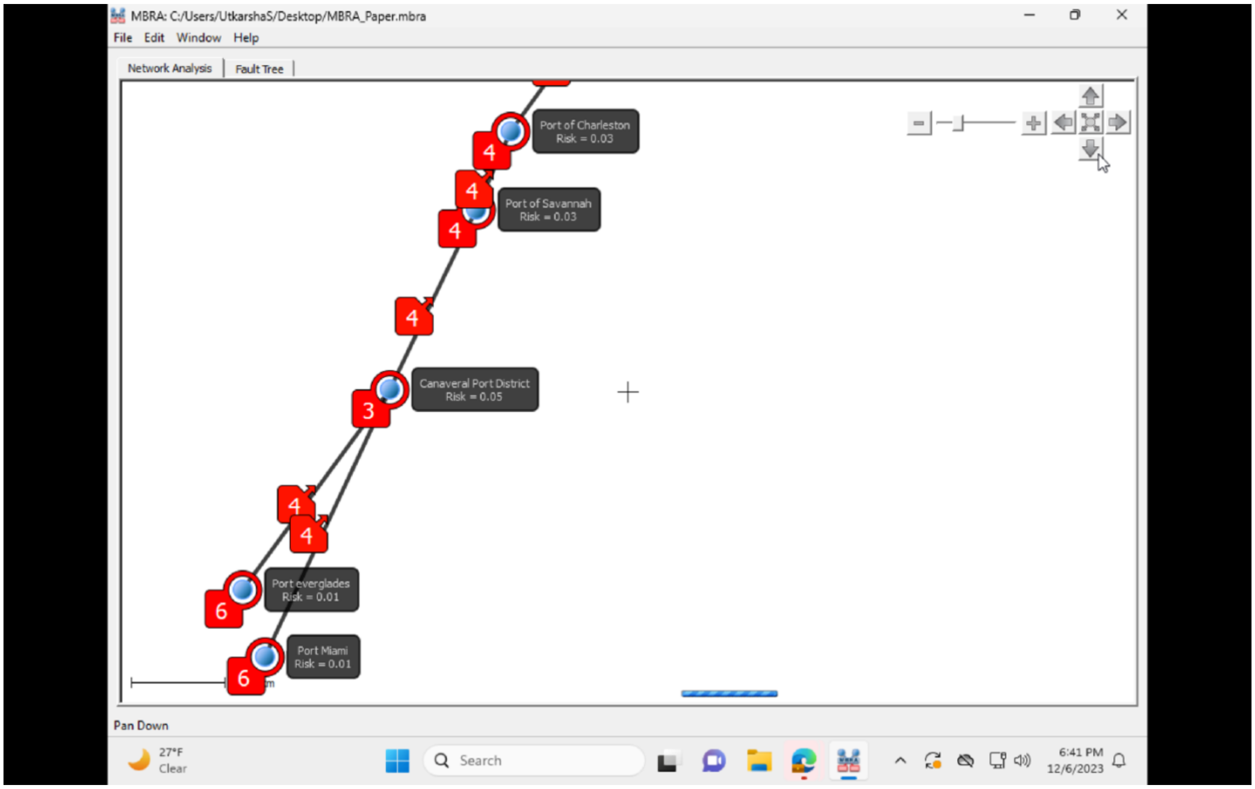
Portland, Maine	A	2	0.142857143	0.005494505	0.184441376
Boston, MA	B	2	0.142857143	0.065934066	0.268702689
Bridgeport, Connecticut	C	2	0.142857143	0.065934066	0.268702689
Port Jefferson, New York	D	1	0.071428571	0	0.205401182
New York City, NY and NJ	E	6	0.428571429	0.576923077	0.598474741
Baltimore, MD	F	2	0.142857143	0	0.356195003
Virginia, VA	G	4	0.285714286	0.604395604	0.439364575
Port Miami, FL	H	1	0.071428571	0	0.00435904
Albany Port District, NY	I	1	0.071428571	0	0.205401182
Richmond, VA	J	1	0.071428571	0	0.15079382
Wilmington, NC	K	2	0.142857143	0.494505495	0.174704005
Port of Charleston, SC	L	2	0.142857143	0.43956044	0.069663921
Port of Savannah, GA	M	2	0.142857143	0.362637363	0.028269225
Canaveral Port District, FL	N	3	0.214285714	0.274725275	0.012696939
Port Everglades, FL	O	1	0.071428571	0	0.00435904





	A	B	C	D	E	F	G
1	Name	Threat	Vulnerability	Consequence	Prevention Cost	Response Cost	
2	Portland, ME	100.00%	50	70	30	5	
3	Boston, MA	100.00%	50	70	30	5	
4	Bridgeport, CT	100.00%	20	70	30	5	
5	Port Jefferson, NY	100.00%	20	60	30	5	
6	New York, NY & NJ	100.00%	90	90	40	10	
7	Baltimore, MD	100.00%	50	70	30	5	
8	Virginia, VA, Port of	100.00%	90	90	40	10	
9	PortMiami, FL	100.00%	20	50	20	4	
10	Albany Port District, NY	100.00%	20	50	30	5	
11	Richmond, VA	100.00%	20	50	30	5	
12	Wilmington, NC	100.00%	50	70	30	10	
13	Port of Charleston, SC	100.00%	50	70	30	5	
14	Port of Savannah, GA	100.00%	50	70	30	5	
15	Canaveral Port District, FL	100.00%	90	80	30	9	
16	Port Everglades, FL	100.00%	20	50	20	4	
17							


MBRA: C:/Users/UtkarshaS/Desktop/MBRA_Paper.mbra
File
Edit
Window
Help
Network Analysis
Fault Tree
Albany Port
Risk = 0.01
Portland, Maine
Risk = 0.03
Boston, MA
Risk = 0.03
Risk = 0.01
Port Jefferson
Risk = 0.01
York
.05
Baltimore
Risk = 0.03
Richmond Port
Risk = 0.01
Virginia
Risk = 0.05
Wilmington
Risk = 0.03
1000 km
6
4
4
4
5
4
4
4
6
4
1
4
4
4
6
4
4
2
4
4
27°F
Clear
Search
6:40 PM
12/6/2023


MBRA: C:/Users/UtkarshaS/Desktop/MBRA_Paper.mbra
File
Edit
Window
Help
Network Analysis
Fault Tree
Port of Charleston
Risk = 0.03
Port of Savannah
Risk = 0.03
Canaveral Port District
Risk = 0.05
Port everglades
Risk = 0.01
Port Miami
Risk = 0.01
4
4
4
4
3
4
4
6
6
Pan Down
27°F
Clear
Search
6:41 PM
12/6/2023