Draft Paper – LNG Export from USA to Europe

Submitted to Secretary of DHS

Nutalapati Avinash

nutalapati.a@northeastern.edu

CY5250 – Decision Making in Critical Infrastructure

Prof. Themis Papageorge

December 2022

Table of Contents

LNG Export from USA to Europe

Introduction to the topic

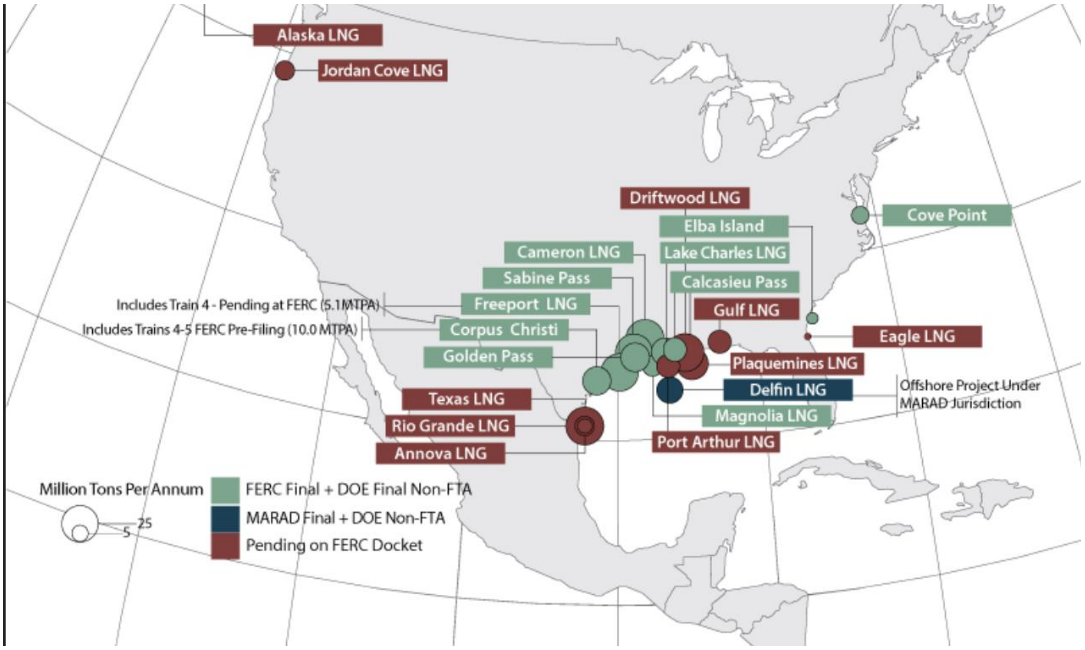
During the first half of 2022, the United States overtook other countries as the greatest exporter of liquefied natural gas (LNG)[1]. LNG is important in the current geopolitical landscape. After Nord Stream was destroyed, the United States stepped in to support NATO nations and allies by supplying natural gas in liquid form to preserve the bilateral relationships within NATO and prevent its destabilization by outside forces. Additionally, assist European nations in battling the energy crisis, which is expected to hit in the winter of 2023, according to government predictions. The residents of numerous European nations have already been asked to consume less electricity due to power outages. Given the background, it is apparent that the supply of LNG is a vital component of the country's infrastructure in the financial and energy sectors. While enabling the USA to increase its revenue through the export of natural resources, LNG also assists in resolving a significant energy dilemma faced by its allies, who are crucial in thwarting the biggest threat to the USA. Any threat to LNG supplies might cause concern among NATO members, disrupt the treaty, and lead to "Rouble" supremacy in the global economy.

LNG plays a role in NATO by providing a secure and reliable source of energy for member states. NATO supports the development of LNG infrastructure and infrastructure projects, such as the construction of LNG terminals and pipelines, to increase energy security and reduce dependence on Russian gas. LNG also provides an alternative to traditional fossil fuels, helping NATO member states to meet their emissions reduction goals and transition to cleaner energy sources. The rise of LNG exports in recent years has been partially due to the ongoing war in Ukraine and the destruction of the Nord Stream pipeline. The war in Ukraine has disrupted the flow of Russian gas through Ukraine, causing concern among European countries about their energy security and leading them to look for alternative sources of natural gas. The destruction of the Nord Stream pipeline has also reduced the amount of Russian gas available to European countries, further increasing demand for LNG. Within context of the larger energy market, this paper discusses LNG manufacturing and supply.

LNG is produced by cooling natural gas to -162°C (-260°F), at which point it becomes a liquid that can be easily transported by tanker ships or trucks. LNG is commonly used as a clean, efficient, and relatively inexpensive fuel for heating, cooking, and generating electricity. The manufacturing of LNG involves a number of steps, including the extraction of natural gas from underground deposits, the purification of the gas to remove impurities, and the cooling and liquefaction of the gas. The LNG is then stored in tanks at the production facility until it is ready to be transported to its destination. LNG transportation involves the movement of liquefied natural gas (LNG) from production facilities to storage and distribution terminals. LNG is transported in specialized ships called LNG carriers, which are equipped with insulation and cryogenic systems to maintain the low temperature and pressure required to keep the gas in a liquid state. LNG is typically transported over long distances, often across oceans, and can be delivered to various terminals for storage and distribution to end users. LNG transportation risks, threats, and vulnerabilities include potential accidents or spills during transport, sabotage or terrorism, and vulnerabilities in the infrastructure or supply chain. These risks can lead to damage to property and the environment, as well as disruptions in the supply of LNG. To mitigate these risks, LNG transportation companies implement safety measures and emergency response plans, and governments regulate the industry to ensure compliance with safety standards.

[1] The United States became the world's largest LNG exporter in the first half of 2022. Homepage - U.S. Energy Information Administration (EIA). (n.d.). Retrieved November 30, 2022, from https://www.eia.gov/todayinenergy/detail.php?id=53159

LNG Production in USA:

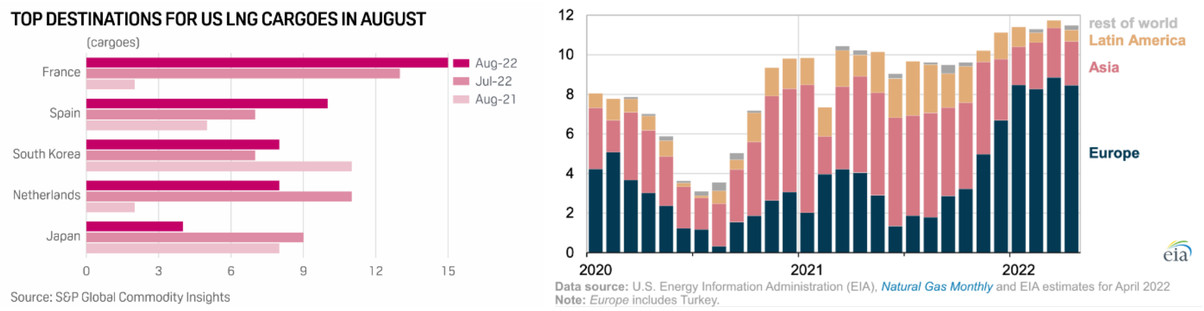


Liquefaction

Liquefaction is the process of converting natural gas into a liquid form, which greatly reduces its volume and makes it easier to transport. However, this process is energy-intensive and can raise the initial price of LNG. Large export terminals that use a network of turbines to chill the natural gas to cryogenic temperatures are the most effective at producing LNG. Small-scale liquefaction is also possible, but it is typically more expensive and less effective. Facilities that are able to liquefy natural gas can store it as LNG and sell it to other facilities, such as those that stockpile supply during peak periods away from the pipeline network. In order to produce LNG, both a natural gas source and the ability to liquefy the gas are required.

Flow of LNG to Other countries network graph and its characteristics

Export of LNG from US to Other countries: (Top 5)


TOP DESTINATIONS FOR US LNG CARGOES IN AUGUST

Source: S&P Global Commodity Insights

Data source: U.S. Energy Information Administration (EIA), *Natural Gas Monthly* and EIA estimates for April 2022
Note: *Europe* includes Turkey.

LNG Exports from USA to other countries

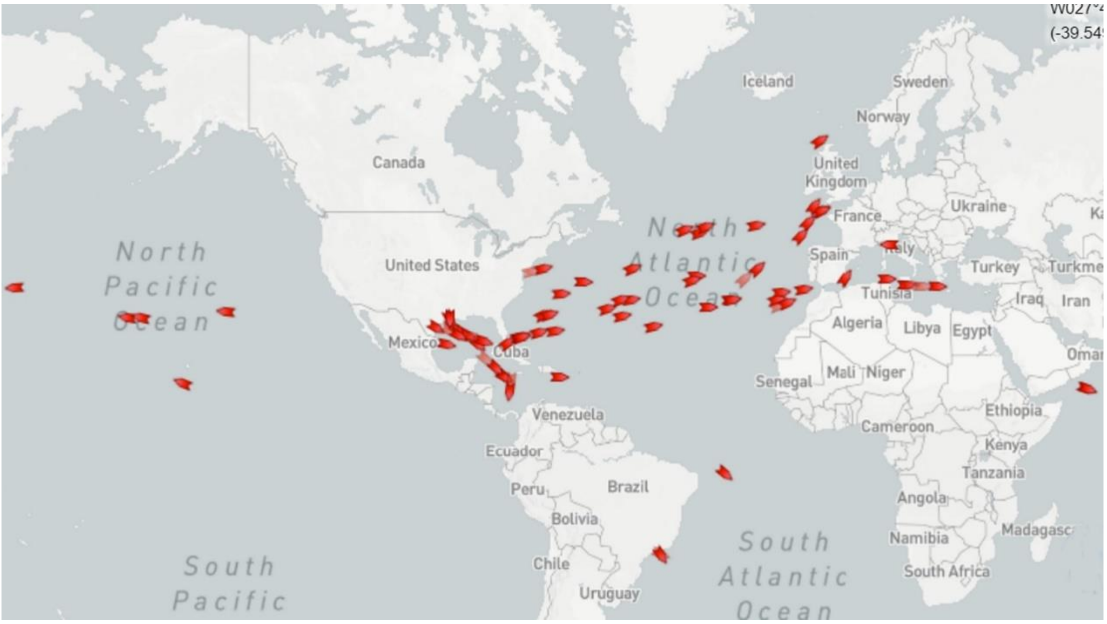
LNG Tanker Ships

LNG tankers are large, specialized ships that are used to transport LNG from one location to another. In order to maintain the LNG at a safe temperature and prevent leaks during transit, LNG tankers are designed with double hulls and multiple large tanks. As of the time of this writing, there are approximately 200 LNG tankers in operation worldwide, with a combined cargo capacity of almost 23 million cubic meters of LNG. This is more than eight times the average daily natural gas consumption in the United States. It is anticipated that more than 200 additional LNG tankers will enter service by 2019. Currently, there are no LNG tankers with American flags.

LNG Marine Terminals

LNG is typically stored and processed at specialized marine terminals before being distributed to domestic markets. These terminals typically consist of docks, LNG processing machinery, storage tanks, and connections to nearby gas pipelines. The Federal Energy Regulatory Commission is responsible for overseeing the location of onshore LNG import terminals in the US. There are relatively few operational inland LNG facilities in the US. For example, the Everett terminal in Massachusetts receives around 65 LNG shipments per year, while the Quintana Island terminal in Texas has the capacity to accept around 200 ships annually.

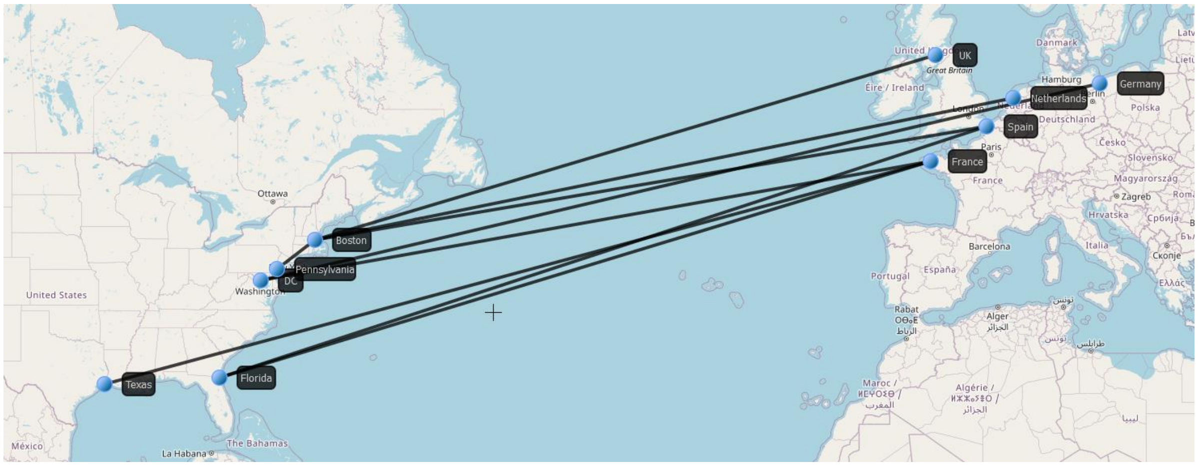
LNG Shipment to Europe from USA – Network Characterization



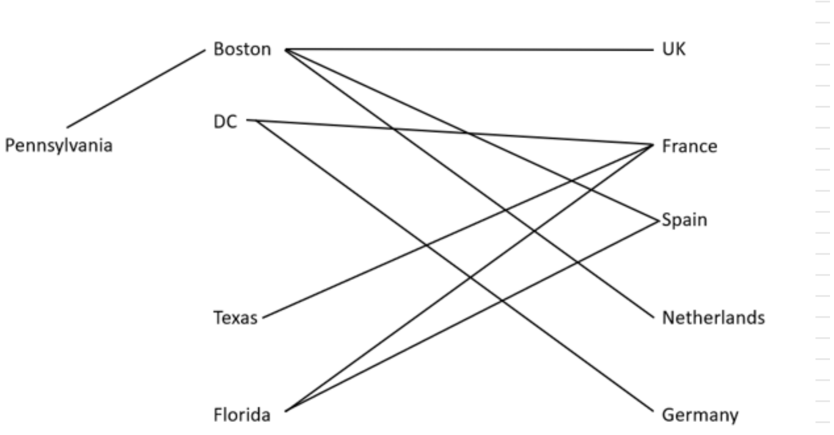
LNG Peak Shaving Plants

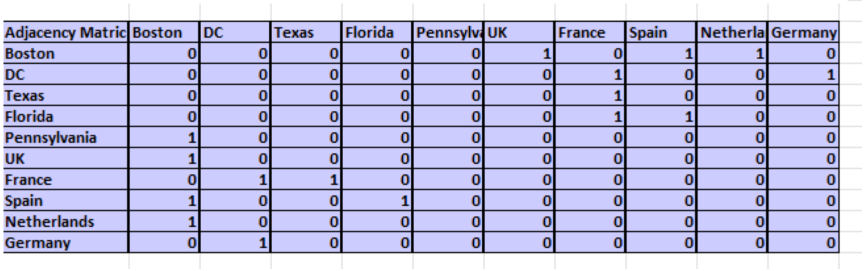
LNG peak shaving plants are facilities that are used to store and regasify liquefied natural gas (LNG) in order to provide a source of natural gas during periods of peak demand. These plants are typically located near major gas consumption centers, such as cities, and are used to supplement the natural gas supply during times of high demand, such as during cold winter months. LNG peak shaving plants can help to ensure a reliable and stable supply of natural gas and can also help to reduce the risk of natural gas shortages and price spikes. There are several LNG peak shaving plants in the US, including plants in Massachusetts, Texas, and Louisiana. During moments of peak usage during wintertime cold snaps, most gas transmission providers depend on "peak shaving" LNG plants that supplement pipeline gas supplies. Large refrigeration tanks connected to the regional gas pipelines are used to store the LNG. While many smaller facilities lack such liquefaction capabilities and instead receive LNG by truck, the biggest plants often liquefy natural gas supplied directly from the interstate pipeline grid. In most cases, containment impoundments are built around LNG tanks to prevent spills and to reduce the potential amount of vapor cloud that could ensue. Although many are in isolated locations far from people, LNG peak shaving terminals are frequently situated close to the populations they serve. There are 103 active pipelines, based on the Pipeline and Hazardous Materials Safety Administration (PHMSA).

LNG Network from USA to European Countries



Adjacency matrix





Adjacency Matric	Boston	DC	Texas	Florida	Pennsylva	UK	France	Spain	Netherla	Germany
Boston	0	0	0	0	0	1	0	1	1	0
DC	0	0	0	0	0	0	1	0	0	1
Texas	0	0	0	0	0	0	1	0	0	0
Florida	0	0	0	0	0	0	1	1	0	0
Pennsylvania	1	0	0	0	0	0	0	0	0	0
UK	1	0	0	0	0	0	0	0	0	0
France	0	1	1	0	0	0	0	0	0	0
Spain	1	0	0	1	0	0	0	0	0	0
Netherlands	1	0	0	0	0	0	0	0	0	0
Germany	0	1	0	0	0	0	0	0	0	0

Using node analysis, we can now evaluate the network and determine its degree, spectral radius, node robustness, blocking nodes and link robustness. Using a Python program, you can calculate the total number of links. Also determine the network degree, & node degree. Once the adjacency matrix is made based on the Network graph of the LNG export, now each node degree and Mean Degree of the Network are determined. Below are the values of the Node degrees. Overall, these terms are used to describe and analyze the structure and connectivity of networks,

A python script is used to determine the below values:

Node degrees

The node degree of a network is a measure of the number of connections or edges that are incident to a given node. In other words, it is a measure of how many other nodes are directly connected to a given node.

Degree of Boston = 3; Degree of DC = 2; Degree of Texas = 1; Degree of Florida = 2; Degree of Pennsylvania = 1; Degree of UK = 1; Degree of France = 2; Degree of Spain = 2; Degree of Netherlands = 1; Degree of Germany = 1;

In the above results, you could observe that the Degree of Boston is more when compared to the other Nodes. Hence the Degree of Network is the highest of the Node degrees, hence

Degree of Network = 3

Mean Degree

The mean degree of a network is a measure of the average number of connections or edges per node in the network. It is calculated by dividing the total number of edges in the network by the total number of nodes.

Mean Degree of Network = 1.6
Eigen values are calculated as below:
Eigenvalues of connection matrix C=

```
[ 0.00000000e+00 1.84775907e+00 1.61803399e+00 -1.84775907e+00
 -1.61803399e+00 7.65366865e-01 6.18033989e-01 -7.65366865e-01
 -6.18033989e-01 -7.21021300e-17]
```

The highest of the Eigen values is considered spectral Radius. The degree of effect a particular node exerts on the other nodes is expressed by its eigenvalue. The spectral radius has the maximum positive eigen value. Because self-organized criticality and danger are inversely correlated with spectral radius.

Spectral radius

The spectral radius of a network is a measure of the largest eigenvalue of the adjacency matrix of the network. In other words, it is a measure of the spread or dispersion of the network.
Spectral radius of connection matrix C=
1.8477590650225724
The indicator of network connectivity is the spectral radius. Greater Spectral radius correlates with increased Vulnerability even as attack surface grows.

Degree Centrality

A node's degree centrality, which is measured by the number of links it holds, is a measure of its significance.
Degree centrality is a measure of the number of connections or edges that are incident to a given node. In other words, it is a measure of how many other nodes are directly connected to a given node. A node with a high degree centrality is considered to be important or central in the network, as it is connected to many other nodes.
Degree Centrality of connection matrix C=

{0: 0.4444444444444444, 1: 0.2222222222222222, 2: 0.1111111111111111, 3: 0.2222222222222222, 4: 0.1111111111111111, 5: 0.1111111111111111, 6: 0.3333333333333333, 7: 0.2222222222222222, 8: 0.1111111111111111, 9: 0.1111111111111111}

Betweenness Centrality

Betweenness Centrality, given that the network is directed, is the number of times a node is on the shortest route between other nodes. Betweenness centrality is a measure of the number of shortest paths between pairs of nodes that pass-through a given node. In other words, it is a measure of how often a given node acts as a bridge or intermediary between other nodes in the network. A node with a high betweenness centrality is important or central in the network, as it plays a key role in connecting other nodes.
Betweenness Centrality of connection matrix C=
{0: 0.5833333333333333, 1: 0.2222222222222222, 2: 0.0, 3: 0.5555555555555556, 4: 0.0, 5: 0.0, 6: 0.5555555555555556, 7: 0.5555555555555556, 8: 0.0, 9: 0.0}

Eigenvector Centrality

In the context of network analysis, eigenvector centrality is calculated by taking the eigenvector of the adjacency matrix of the network, where the elements of the matrix represent the connections or edges between the nodes in the network. The eigenvector centrality of a given node is then calculated by summing the elements of the eigenvector that correspond to that node.

A node with a high eigenvector centrality is important or central in the network, as it is connected to many other important or central nodes. In other words, eigenvector centrality considers not only the number of connections a node has, but also the importance of the nodes it is connected to. It is based on the concept of eigenvectors, which are vectors that do not change direction when multiplied by a matrix.
Eigenvector Centrality of connection matrix C=
{0: 0.56722198861688, 1: 0.18966442039241496, 2: 0.1485339200392267, 3: 0.3467337564537116, 4: 0.2641448333874958, 5: 0.26414483338749584, 6: 0.3189602629028713, 7: 0.4256123578599077, 8: 0.2641448333874957, 9: 0.08832322746558548}

Link Robustness

The number of links that can be withdrawn from a network without it breaking up into disconnected parts is known as link robustness. Although link robustness boosts a network's resilience, it also causes SOC, which raises vulnerability. It serves as a nice illustration of the redundancy paradox.
$\kappa L = (m-n)/m$
m = number of links, n = number of nodes
$\kappa L= 9-10/10=-0.1$
The Links that cannot be removed are Pen – Boston link as the major LNG transportation by road happens through this. The removal of this link would sabotage the whole LNG supply within the country to New England and other countries as well.

Node Robustness

This gauges the number of nodes that can be eliminated in order to divide a network structure into its component parts. In general, spectral radius increases node robustness.
$\kappa N = 1-1/\rho$
λ = mean degree, ρ = spectral radius.
The Node that cannot be removed is Boston node as the major LNG transportation by road happens through this. Boston is considered as the critical node given its state of importing LNG from various parts of the country and exporting it to various countries. Boston is the crucial node of LNG supply to New England areas.

Blocking Nodes

If indeed the removal of a node results in a disconnect, those nodes are said to be blocking nodes. Betweenness and the spectral radius both rise as the number of links and node connectivity do. The nodes that block traffic are those that become disconnected islands when a node is removed from the network.
Blocking nodes are necessary to maintain network connectivity.
Blocking Nodes = n/ρ apprx.
n = number of nodes, ρ = spectral radius
Blocking Nodes = 10/1.84 = 5.43
Hence there are approximately 5 Blocking nodes out of 10 nodes in the LNG export network.

Random and Targeted attacks

Random attacks on LNG tankers could include incidents such as acts of piracy or terrorism, where the attacker does not have a specific target or motive, but is simply looking to cause disruption or damage. For example, a group of pirates could attack an LNG tanker in the open sea in order to steal its cargo or ransom its crew.

Targeted attacks on LNG tankers, on the other hand, could involve attackers who have a specific target or motive for their attack. For example, a terrorist group could attack an LNG tanker that is known to be carrying LNG from the US to Europe in order to disrupt the supply of LNG to Europe and create economic and political instability.

Also, Refer figure 1.8 in Appendix for Attack map on LNG.
LNG Risks and Vulnerabilities:
There has been discussion about LNG terminal safety risks for many years. 128 people were killed in a 1944 disaster at one of the country's first LNG facilities, which also sparked public apprehension about the dangers of LNG that still exist today. Since the 1940s, technological advancements and standards have greatly increased the safety of LNG facilities, but because LNG is inherently flammable and is transported and stored in enormous amounts, substantial risks still exist. The ongoing debate over LNG facility safety was exacerbated in January 2004 by an incident at Algeria's Skikda LNG unit that resulted in over 100 worker fatalities or injuries. The LNG infrastructure might also be attacked by terrorists.

LNG Security Risks

Facilities on land and LNG tankers may be at risk from terrorism. Alternatively, tankers might be taken over and used as weaponry against coastal locations after being violently attacked to damage their cargo. Explosives or other methods could also be used to physically harm land-based LNG facilities. As an alternative, computer control systems may be "cyber-attacked," or a simultaneous physical and cyberattack may take place. Other terrorist attacks such as those on local power grids or communication networks, which in turn could have an impact on LNG safety and control systems, could also indirectly impair some LNG plants. Due to its use as fuel for military facilities, power plants, and other applications, LNG offers significant "downstream" dangers, particularly in places that depend more heavily on it, like NewEngland.

One key risk to consider is the potential for accidents or incidents during the transportation of LNG. LNG is a highly flammable and volatile substance, and as such, there is always a risk of accidents or incidents occurring during transportation. This could include spills, leaks, or fires, all of which could have significant consequences for human health and the environment. Another key risk to consider is the potential for damage to the environment. LNG is a fossil fuel, and its extraction and transportation can have negative environmental impacts. This could include air and water pollution, as well as the potential for greenhouse gas emissions. Additionally, the construction of LNG facilities and infrastructure can also have environmental impacts, such as habitat destruction and disruption to ecosystems.

Another significant risk to consider is the potential economic and political risks associated with exporting LNG to Europe. The global market for LNG is highly competitive, and there is always the potential for changes in market conditions or shifts in political dynamics that could impact the profitability of LNG exports to Europe. Additionally, there may be political risks associated with exporting LNG to certain European countries, depending on the specific geopolitical context.

Other Threats and Attacks

- Elevated geopolitical risk,
- Terrorism: Inflation – could affect base rates.
- Pool fires
- Flammable vapor clouds
- Flameless explosion
- Cyber Attacks on Production plants (Marcellus and Utica, black shale, Cheniere Energy formations in Ohio, West Virginia, Pennsylvania, and Houston);
- Physical or Cyber-attacks on container Tanker ships (Missile attack from Submarines/Warships/Fighter Jet and Satellite/Radio communications disruption);
- Radioactive exposure for US and European workers caused by LNG;
- Pool fires, Flameless explosion and formation of Flammable vapor clouds;
- LNG leakage in Atlantic Ocean or US/European soil; Australia, China, and Qatar LNG Supply; Any kind of damage to US import of LNG from Trinidad and Tobago.

Values used for Threat Probabilities, Vulnerability Probabilities, Consequences, Prevention Costs, and Response Costs.

The values used for Threat Probabilities, Vulnerability Probabilities, Consequences, Prevention Costs, and Response Costs in the mbra tool for LNG maritime security would depend on the specific risks and vulnerabilities being analyzed, as well as the organization's specific security objectives and priorities.

Threat Probabilities would typically be based on the likelihood of different types of threats to the LNG transportation system, such as piracy, terrorism, or natural disasters. These probabilities could be determined through a combination of expert judgment, data analysis, and scenario-based modeling.

Vulnerability Probabilities would reflect the likelihood that a specific vulnerability could be exploited by a threat, given the organization's current security measures and controls. These probabilities could be determined through a combination of expert judgment, data analysis, and vulnerability assessments.

Consequences would refer to the potential impact of a threat exploiting a vulnerability, such as financial losses, damage to reputation, or loss of life. These consequences could be quantified in terms of their expected value, using data on historical losses, industry benchmarks, and expert judgment.

Prevention Costs would refer to the costs associated with implementing security measures and controls to prevent threats from exploiting vulnerabilities, such as personnel expenses, equipment costs, and training expenses. These costs could be estimated based on the organization's existing security budget and the costs of implementing different security measures and technologies.

Response Costs would refer to the costs associated with responding to a threat that has already exploited a vulnerability, such as emergency response expenses, cleanup costs, and compensation expenses. These costs could be estimated based on the organization's existing emergency response plan and the costs of implementing different response measures and technologies.

The threats and vulnerabilities to LNG transportation were analyzed using data from the internet and knowledge from a Security Risk Assessment course. The probabilities of threats and vulnerabilities were determined, and a budget was calculated for rebuilding damaged tankers, addressing the consequences of an attack, and preventing and responding to attacks. LNG tanker and shipping rates were considered in the budget calculation.

Charter rates for LNG tankers are currently trading near their highest level in a decade, at $120,000 per day. LNG carriers have increased in size over the years, with the newest generation of ships being 216,000 to 266,000 cubic meters. These large ships can carry around 6 billion cubic feet of gas, equivalent to one day's average consumption for the UK or around 10% of the US' daily gas production. A newly built LNG carrier is estimated to cost $200-250 million, which would require a charter rate of $80,000-$100,000 per day to cover capital and operating costs. However, current spot charter rates are only a third or a quarter of these levels, making it difficult for ships without long-term charter arrangements to find economically viable short-term charters.

Uncertainty About LNG Threats

Since September 11, 2001, there has been discussion about the possibility of a terrorist assault on the infrastructure supporting the U.S. LNG industry. No LNG ship or ground LNG facility has indeed been damaged by terrorists to this point. Similar gas and oil installations, however, have been popular terror targets across the globe. For instance, since 2001, pipelines carrying gas and oil have indeed been targeted in at least six different nations. A fishing boat carrying bombs attacked the French tanker truck Limburg in October 2002 off the coast of Yemen. U.S. intelligence agencies issued a warning about potential Al Qaeda strikes on Texas oil installations in June 2003. In its list of fifteen potential threats, the Homeland Security Council listed terrorist attacks on "freight ships" transporting "flammable substances."

Given the current geopolitical scenario and uncertainty of threats, Threat Probability is considered as 100%.

LNG Tanker Vulnerability

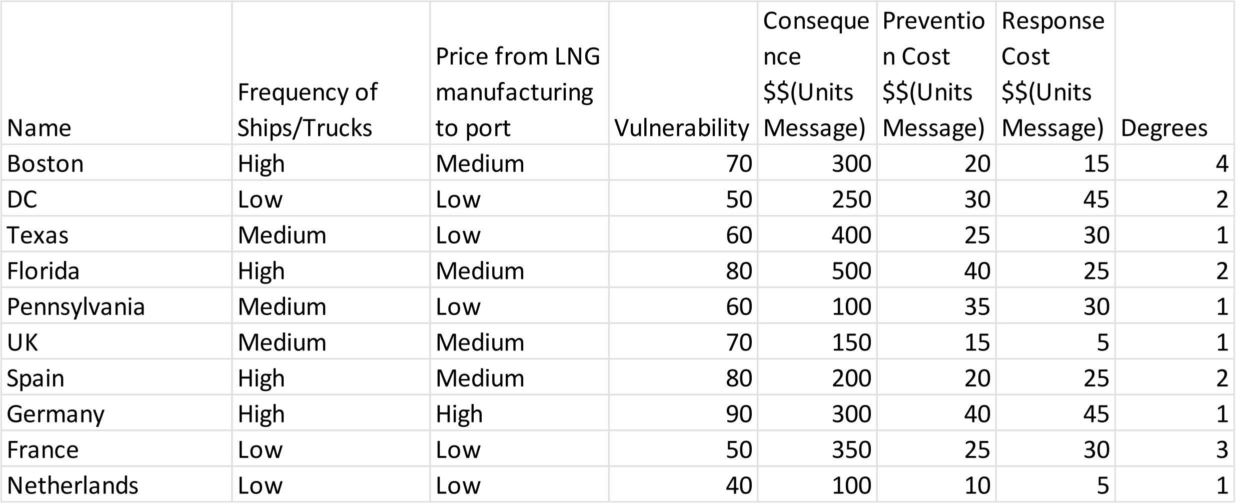
Security analysts are most concerned about LNG tankers since they could be more approachable than fixed terminals, they may pass through more densely populated regions, and LNG leaks from tankers may be more challenging to contain. An intentional LNG spill and ensuing fire, according to a 2004 Sandia National Laboratories report, could result in "major" injury issues to individuals and "significant" structural damage within 500 meters (0.3 miles) of the point of discharge, more modest injuries, and structural failure to 1,600 meters (1.0 miles), and lower affects out with 2,500 meters (1.5 miles). Federal authorities use these findings while evaluating LNG terminal siting requests.

Vulnerability Probability values are determined as follows:
Based on the qualitative analysis of Frequency of Ships/Trucks/Rails of LNG transportation and Price of transportation of LNG from manufacturing plant to Port and then to other countries. Also, in accordance with attacks happened till date, most weakly secured areas.

Name	Frequency of Ships/Trucks	Security Measures applied	Vulnerability
Boston	High	Medium	70
DC	Low	Low	50
Texas	Medium	Low	60
Florida	High	Medium	80
Pennsylvania	Medium	Low	60

UK	Medium	Medium	70
Spain	High	Medium	80
Germany	High	High	90
France	Low	Low	50
Netherlands	Low	Low	40
Pen - Bos - Rail	High	High	95
Bos - Uk - Ship	High	High	95
Flo - Fra _ Ship	High	High	95
Tex - Fra - Ship	High	High	95
Bos - Spain - Ship	High	High	95
Bos - Net - Ship`	High	High	95
DC - Germany - Ship	High	High	95
Flo - Spain - Ship	High	High	95
Dc- Fra - Ship	High	High	95

Consequences values are determined as follows:
Based on the amount of LNG being carried by the tankers/trucks and the current price of the LNG manufacturing were calculated in a qualitative method.



Name	Frequency of Ships/Trucks	Price from LNG manufacturing to port	Vulnerability	Consequence $$(Units Message)	Prevention Cost $$(Units Message)	Response Cost $$(Units Message)	Degrees
Boston	High	Medium	70	300	20	15	4
DC	Low	Low	50	250	30	45	2
Texas	Medium	Low	60	400	25	30	1
Florida	High	Medium	80	500	40	25	2
Pennsylvania	Medium	Low	60	100	35	30	1
UK	Medium	Medium	70	150	15	5	1
Spain	High	Medium	80	200	20	25	2
Germany	High	High	90	300	40	45	1
France	Low	Low	50	350	25	30	3
Netherlands	Low	Low	40	100	10	5	1

To calculate the current LNG price, the below formula is used:

Oil Indexed Price Formula

The oil indexed price formula for LNG is a pricing mechanism used to determine the price of LNG based on the price of oil. This formula is commonly used in long-term LNG supply contracts, where the price of LNG is linked to the price of oil. The formula typically involves multiplying the price of oil by a fixed conversion factor to determine the price of LNG. This conversion factor can vary depending on the specific contract and the relative energy content of LNG compared to oil. The use of an oil indexed price formula for LNG allows the price of LNG to fluctuate based on the market price of oil, providing a mechanism for managing price risk and ensuring a fair price for both the buyer and the seller.

Approximately 70% of the global LNG trade is priced using a competing fuels index, which is typically based on crude oil or fuel oil. This pricing mechanism is commonly referred to as "oil price indexation" or "oil-linked pricing." In the Asia-Pacific region, LNG contracts are often based on the Japan Customs-cleared Crude Oil (JCC) index, due to the historical linkage between LNG trade and oil-based power generation in Japan. Most LNG contracts in the Asia-Pacific region that were developed in the late 1970s and early 1980s use a formula that can be expressed as follows: [LNG price] = [JCC price] x [conversion factor].

$P = \alpha \text{ x } P + \beta$

Where:

PLNG = price of LNG in U.S.$/mmBtu (U.S.$/GJ x 1.055)

α = crude linkage slope

Pcrude = price of crude oil in U.S.$/barrel

β = constant in U.S. $mmBtu (U.S.$GJ x 1.055)

Along with LNG price, the hazards it may cost in the sea, pollution damages and its fines are also considered in determining the consequence costs.

Name	Vulnerability	Consequence $$
Boston	70	300
DC	50	250
Texas	60	400
Florida	80	500
Pennsylvania	60	100
UK	70	150
Spain	80	200
Germany	90	300
France	50	350
Netherlands	40	100

Prevention Costs, and Response Costs

Along with the LNG price, Container costs and Loss of Revenue, the budget required to perform security risk assessments and add the recommended controls were considered.

Name	LNG Costs, Container costs, Loss of Revenue	Prevention Cost $$(UnitsMessage)	Response Cost $$(Units Message)
Pen - Bos - Rail	Low	10	5
Bos - Uk - Ship	Medium	50	25
Flo - Fra _ Ship	High	60	30
Tex - Fra - Ship	High	70	35
Bos - Spain - Ship	Medium	40	20
Bos - Net - Ship`	High	65	30
DC - Germany - Ship	Medium	55	25
Flo - Spain - Ship	High	60	30
Dc- Fra - Ship	Low	40	20

MBRA tool is used to estimate Risks and Critical Nodes. Refer figure 1.7 for Data table of MBRA tool. Refer figure 1.6 for network map made using MBRA tool.

Proposed Risk Prevention and Response Controls

In order to prevent and respond to risks associated with the export of LNG, it is important to implement a range of risk prevention and response controls. Some potential controls that could be implemented include:

1. **Develop and implement a comprehensive security plan**: In order to prevent and respond to security risks associated with LNG export, it is essential to develop and implement a comprehensive security plan. This plan should identify the specific security risks and hazards associated with LNG export, and outline the measures that will be taken to mitigate or manage these risks. This could include implementing security protocols and procedures, conducting security assessments and audits, and implementing security technologies and systems.
2. **Train and educate employees**: In order to prevent and respond to security risks associated with LNG export, it is essential to train and educate employees on security best practices and procedures. This could include providing regular training on security protocols, conducting security drills and exercises, and promoting a culture of security within the organization.
3. **Conduct regular security assessments and audits**: In order to identify and address potential security vulnerabilities, it is essential to conduct regular security assessments and audits of LNG export facilities and infrastructure. This could include conducting physical security inspections, testing security systems and technologies, and conducting vulnerability assessments.
4. **Implement security technologies and systems**: In order to prevent and respond to security risks associated with LNG export, it is essential to implement security technologies and systems. This could include installing security cameras, implementing access control systems, and deploying security software and systems to monitor and detect potential security threats.

The LNG cargoes that are shipped to the Everett port are the most tightly secured, as they pass through Boston harbor. Depending on the level of alert, the Coast Guard and local law enforcement agencies may implement a range of security measures for these shipments, including:

- Security inspections and tanker loading at the points of entry
- On-board security from Boston provided by Coast Guard "sea marshals"
- 96 hours' notice prior to the arrival of an LNG tanker
- Prior notice to the Federal Aviation Administration, the U.S. Navy, and local emergency response agencies
- Boarding LNG ships before they reach Boston Harbor for inspection
- Marines escorting the harbor in armed cutters or support vessels
- Establishing a safety zone that is two

The Coast Guard asserts that comparable security procedures have been put in place for those other U.S. LNG facilities, depending on regional assessments of any possible threat and the unique characteristics of each marine area.

Overall, by implementing these risk prevention and response controls, organizations can effectively prevent and respond to security risks associated with the export of LNG.

Required budget for risk mitigation and resilience improvement.

The required budget for risk mitigation and resilience improvement of LNG exports security will depend on a range of factors, including the specific risks and vulnerabilities that need to be addressed, the size and complexity of the LNG transportation system, and the level of investment and resources that are required to implement the necessary security measures.

However, organizations involved in LNG transportation should carefully evaluate their risks and vulnerabilities and develop a budget and plan for addressing these risks and improving resilience. This budget and plan should be based on a thorough assessment of the potential costs and benefits of implementing different security measures and technologies, as well as the potential risks and consequences of not implementing such measures.

At Boston, the criticality is higher as it has many Peak shavers, and most of the exports happen from Massachusetts. Also, From Pennsylvania and other parts of the country, LNG transfers to Massachusetts. Risk Prevention and Response cost will decide the budget for Risk Mitigation and Risk Resilience. As the LNG manufacturing and Transportation costs were discussed in the above, the range of prevention and response costs is $5M to $50M.

Resilience equation and Critical vulnerability

The critical vulnerability is during the ships' passage towards Europe, where the coast guard security is less and there is a high possibility of marine attacks and cyber-attacks on the ships.

$$\sum_i R = T \sum_i gVC$$

Equation for Basic Resilience: q = 10b+k*ro*gamma the variables b and k.
Gamma: Single node susceptibility
spectral radius is (ro)

The resilience equation is a mathematical formula used to assess the resilience of a system or network. It is based on the idea that resilience is the product of the system's ability to absorb shocks or disturbances (absorptive capacity), its ability to adapt and recover from shocks or disturbances (adaptive capacity), and its ability to prevent or reduce the likelihood of shocks or disturbances (preventive capacity).

In the context of LNG transportation, the resilience equation could be used to assess the resilience of the transportation infrastructure and systems. This could involve evaluating the absorptive, adaptive, and preventive capacities of the infrastructure and systems, and using the resilience equation to calculate the overall resilience of the system.

When q = 1, the critical vulnerability probability, also known as the infectiousness point, is reached, and log(q) = 0. CIKR is at greater risk when the main gamma is higher than the gamma. If it is high, a complicated catastrophic risk exists.

Risk equation for risk to network with i nodes, g=node degree. Threat (T) is generic threat to network.
For vulnerability 10%:
q1 = $10^{b+k\gamma\rho}$
$\gamma=10\%; \rho=1.84; q1=1.88$

log(q1) = $b+k\gamma\rho$
For vulnerability 90%:
q2 = $10^{b+k\gamma\rho}$
$\gamma=90\%; \rho=1.84; q2=0.4$

where b,k are constants, b=0.395, k=-0.0067

Critical Vulnerability (γ0):

Critical vulnerabilities are specific vulnerabilities or weaknesses that could compromise the integrity, reliability, or availability of a system or network. In the context of LNG transportation, critical vulnerabilities could include weaknesses in the transportation infrastructure, such as inadequate security measures or inadequate maintenance, as well as vulnerabilities in the systems and processes used to transport LNG, such as inadequate training or inadequate emergency response plans.

Overall, the resilience equation and critical vulnerabilities are two important concepts that can be used to assess and manage the risks associated with LNG transportation. By evaluating the resilience of the transportation infrastructure and systems, and identifying and addressing critical vulnerabilities, organizations can ensure the safe and reliable transportation of LNG.
$\gamma 0 = -b/k\rho$, where b, k, and ρ are determined by the topology of the complex CIKR network
$\gamma 0 = -0.395/0.0067*1.84 = 32\%$

When the fractal dimension of its exceedance probability curve ro*gamma > 1, a highly connected, interdependent complex CIKR system transforms from low risk to high-risk, and when ro*gamma >> 1, it changes from a common accident to a complex catastrophe.

ROI: Return on Investment

The return on investment (ROI) of a security budget spent on LNG exports will depend on a range of factors, including the specific security measures and technologies implemented, the risks and vulnerabilities that are addressed, and the potential consequences and costs of not implementing such measures.

In general, the ROI of a security budget spent on LNG exports can be determined by comparing the benefits and savings generated by the security measures (such as avoided losses, reduced insurance premiums, and improved operational efficiency) with the costs of implementing and maintaining the measures (such as personnel, equipment, and training expenses). By carefully evaluating the potential benefits and costs of different security measures, organizations can determine the ROI of their security budgets and make informed decisions about how to allocate their resources.

Total Risk Initial = 4312
Total Risk Reduced = 1512.64
Investment = 260.16
ROI = Risk(before) - Risk(after)/$Investment = 10.760
In the scenario that follows, I'm using the example of a specific electric grid experiencing power interruptions.

The size of each given Network's failures is measured by True Exceedance. When Exceedance Probability EP (x >=X) denotes the likelihood that the size of an event x equals or surpasses X, True Exceedance is considered. The size of the incident is greater when the LNG exports on the highest node are jeopardized.

Exceedance Probability declines as the severity of the effects rises. If there are more shipment issues on the Atlantic, EP will drop. The shape curve of the graph when using simulated or actual data from past occurrences determines the fractal dimension (q). In essence, power laws are straightforward fractals.

There are two types of PML risk: Low Risk and High Risk. As an event gets bigger, the risk goes down. The definition of PML risk is in terms of consequence.

In this scenario, LNG delivery delays resulting from potential threats might be considered. By using Fractal Dimension (q), one may be able to assess the system's criticality considering potential dangers. Cascading is the situation where a node's action on one node also affects nearby nodes. The word used to describe the density of the specified network is spectral radius. High spectral radii are associated with less robust systems.

Fault Tree Analysis

A fault tree analysis is a technique used to identify the potential causes and consequences of a particular failure or event. In the context of critical infrastructure, a fault tree analysis could be used to identify the potential causes of a failure or incident that could impact the reliability and availability of the infrastructure. The MBRA (Model-Based Risk Assessment) tool is a software application that can be used to conduct fault tree analyses. It allows users to create and analyze fault trees, identify potential failure modes and consequences, and evaluate the likelihood and impact of different scenarios.

To conduct a fault tree analysis of critical infrastructure using the MBRA tool, users would first need to identify the specific failure or event that they want to analyze. This could be a failure or incident that has already occurred, or a hypothetical scenario that is being considered. Next, users would need to define the components of the critical infrastructure that are relevant to the analysis and create a fault tree diagram that shows the potential causes and consequences of the failure or event. This could involve identifying the potential failure modes of each component, as well as the likelihood and impact of each failure mode. Once the fault tree diagram has been created, users can use the MBRA tool to analyze the diagram and evaluate the overall likelihood and impact of the failure or event. This could involve simulating different scenarios and exploring the potential consequences of different failure modes. Overall, a fault tree analysis using the MBRA tool can provide valuable insights into the potential causes and consequences of a failure or incident in critical infrastructure and can help organizations identify strategies for mitigating or managing the risks associated with such events.

Refer Figure 1.11 in Appendix

Vulnerability elimination costs and optimal budget allocations of LNG

One potential example of vulnerability elimination costs and optimal budget allocations for LNG export security analysis could involve addressing the vulnerability of LNG tanker ships to piracy. This vulnerability could be addressed by implementing a range of security measures, such as hiring and training security personnel, installing surveillance and communication equipment, and implementing security protocols for LNG tanker operations. The costs of these measures could include personnel expenses, equipment costs, and training expenses.

To determine the optimal budget allocation for addressing this vulnerability, an organization could conduct a cost-benefit analysis of different security measures, considering the potential risks and consequences of not addressing the vulnerability (such as losses from piracy, damage to reputation, and increased insurance premiums), and the potential benefits and savings of implementing different security measures (such as avoided losses, reduced insurance premiums, and improved operational efficiency). Based on this analysis, the organization could determine the most cost-effective way to allocate its security budget to different vulnerability elimination activities.

For example, the organization could determine that hiring and training security personnel is the most cost-effective way to address the vulnerability of LNG tanker ships to piracy and allocate a significant portion of its security budget to this activity. It could also allocate a smaller portion of its budget to purchasing and installing surveillance and communication equipment and implementing security protocols for LNG tanker operations. By carefully considering the potential risks and consequences of not addressing specific vulnerabilities, and the potential benefits and savings of implementing different security measures, the organization can determine the optimal budget allocation for addressing the vulnerability of LNG tanker ships to piracy.

Critical Nodes

Critical node cities in the LNG export from the US could include major export terminals. Most critical Node is considered as Boston. LNG export terminals are important because they facilitate the movement of LNG from the production site to the point of consumption. This is particularly important for LNG exports from the US to Europe, as the US has significant reserves of natural gas but is geographically distant from major European markets. LNG export terminals in the US, such as the one in Boston, provide a crucial link in the supply chain, allowing the US to export its natural gas to Europe and other markets.

In addition to facilitating trade, LNG export terminals also provide economic benefits to the local communities where they are located. For example, the LNG export terminal in Boston creates jobs and generates economic activity in the region. It also provides a source of revenue for the state and local governments through taxes and other fees.

The 2nd highest critical node is considered Texas. The LNG export terminal in Texas is important because it is a major hub for the export of LNG from the US. The terminal, which is located in Quintana Island in Brazoria County, has the capacity to accept around 200 ships per year and is a key link in the supply chain for LNG exports from the US to Europe and other destinations.

Texas is a leading producer of natural gas in the US, and the LNG export terminal in Quintana Island plays a critical role in enabling the state to access global markets for LNG. The terminal allows Texas to take advantage of its abundant natural gas resources and increase its exports of LNG, which can generate significant economic benefits for the state. In addition to its economic importance, the LNG export terminal in Texas also has strategic importance for the US. The terminal is part of the country's overall energy infrastructure and plays a key role in ensuring the security and reliability of the US' natural gas supply. By exporting LNG, the terminal helps to diversify the country's energy sources and reduce its reliance on other forms of energy, such as oil and coal.

Major import terminals in Europe, such as UK & Spain. These countries are critical because they are key hubs for the movement of LNG, and disruptions at these locations could have significant impacts on the overall LNG supply chain.

In the UK, LNG import terminals play a crucial role in providing natural gas to the country's energy mix. The UK has a number of LNG import terminals, including the Isle of Grain terminal in Kent and the Dragon terminal in Wales. These terminals receive LNG shipments from countries such as Qatar and the US, and then regasify the LNG to make it suitable for use in the UK's natural gas grid.

In Spain, LNG import terminals also play a key role in providing natural gas to the country's energy mix. Spain has several LNG import terminals, including the Huelva terminal in Andalusia and the Sagunto terminal in Valencia. These terminals receive LNG shipments from countries such as Qatar and Algeria, and then regasify the LNG to make it suitable for use in Spain's natural gas grid.

Critical link routes in the LNG export from the US could include the shipping routes from the US export terminals to the European import terminals, as well as the pipelines and other infrastructure that connect the export and import terminals. These routes are critical because they are the primary means of transporting LNG from the US to Europe, and disruptions along these routes could have significant impacts on the overall LNG supply chain. Examples of critical link routes could include the route from Sabine Pass to Zeebrugge, or the route from Cove Point to Rotterdam.

Role of NICC/NCICC

The costs of LNG marine security will vary depending on a range of factors, including the specific security measures and technologies that are implemented, the size and complexity of the LNG transportation system, and the level of risk and threat that is being addressed.

Some potential costs of LNG marine security could include:

- The cost of implementing security technologies and systems, such as security cameras, access control systems, and security software.
- The cost of training and educating employees on security protocols and procedures.
- The cost of conducting security assessments and audits.
- The cost of implementing security protocols and procedures, such as security clearance procedures, security screenings, and security drills and exercises.
- The cost of responding to security incidents and breaches, including the cost of investigating and mitigating the impact of the incident.

Overall, the costs of LNG marine security can be significant, but they are necessary to ensure the safe and secure transportation of LNG. Organizations should carefully consider the potential costs of implementing security measures and weigh them against the benefits of improved security and the potential risks and consequences of not implementing such measures. The National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) are both organizations within the US Department of Homeland Security that play a role in the transportation of LNG.

The NICC is responsible for coordinating the protection and resilience of the US critical infrastructure, including the transportation of LNG. This includes working with the LNG industry and other stakeholders to develop and implement best practices and guidance for securing LNG transportation infrastructure, as well as providing training and support to organizations in the LNG industry. The NICC is responsible for providing guidance and support to the US industrial control systems (ICS) community, including the LNG industry. This includes developing and disseminating best practices and guidance for securing industrial control systems, as well as providing training and support to organizations in the LNG industry.

The NCCIC, on the other hand, is a 24/7 cybersecurity operations center that monitor and responds to cyber threats and incidents. This includes providing real-time situational awareness and technical assistance to organizations in the LNG industry, as well as coordinating with other government agencies and private sector partners to mitigate and respond to cyber threats. Overall, the NICC and NCCIC play a critical role in ensuring the safe and secure export of LNG from the US to Europe by providing guidance, support, and response capabilities to the LNG industry.

Work Force Recommendations

In order to ensure the safe and secure export of LNG from the US to Europe, it is important to have a strong and capable cybersecurity workforce in place. Some potential recommendations for building a robust cybersecurity workforce for this purpose include:

1. Invest in training and professional development: In order to stay up to date with the latest threats and best practices in cybersecurity, it is essential to invest in ongoing training and professional development for the workforce. This could include offering training courses, attending conferences and seminars, and providing opportunities for employees to earn professional certifications.
2. Hire and retain top talent: In order to build a strong and capable cybersecurity workforce, it is important to hire and retain top talent. This could involve offering competitive salaries and benefits packages, as well as providing opportunities for career growth and advancement.
3. Foster a culture of cybersecurity: In order to effectively protect against cyber threats, it is important to foster a culture of cybersecurity within the organization. This could involve promoting cybersecurity best practices, regularly conducting cybersecurity drills and exercises, and creating a supportive and collaborative work environment.
4. Collaborate with external partners: In order to stay ahead of cyber threats, it is essential to collaborate with external partners and stakeholders, including other organizations, government agencies, and industry groups. This could involve sharing information and expertise, as well as participating in joint training and exercises.

Overall, by implementing these recommendations, organizations can build a strong and capable cybersecurity workforce that is well-equipped to handle the unique challenges and risks associated with LNG export from the US to Europe. Some other potential cybersecurity roles in an LNG export cybersecurity team are:

1. Cybersecurity Manager: responsible for developing and implementing the overall cybersecurity strategy and policies for the LNG export team.
2. Cybersecurity Analyst: responsible for monitoring and analyzing cyber threats and vulnerabilities and providing recommendations for mitigating risks.
3. Incident Response Coordinator: responsible for coordinating the team's response to cyber incidents and coordinating with relevant stakeholders, such as law enforcement and other government agencies.
4. Cybersecurity Trainer: responsible for providing training and education to team members on cyber threats, best practices, and emergency response procedures.
5. Cybersecurity Engineer: responsible for designing, implementing, and maintaining the technical security controls and systems for the LNG export team.

Tasks for these roles could include:

- Developing and implementing cybersecurity policies and procedures
- Monitoring and analyzing cyber threats and vulnerabilities
- Coordinating the team's response to cyber incidents
- Providing training and education on cybersecurity best practices
- Designing, implementing, and maintaining technical security controls and systems.

OPM Code (Fed Use):-
611, 612, 621, 622, 651, 652, 661, 641, 671, 631, 632, 421, 422, 431, 411, 441, 451, 461, 731, 732, 711, 712, 722, 723, 751, 752, 901, 801, 802, 803, 804, 805, 511, 521, 531, 541, 141, 121, 111, 112, 131, 132, 151, 311, 312, 331, 332, 333, 321, 221, 211, 212.

The above-mentioned job roles must be filled wherever needed, from LNG manufacturing units to delivery and dispatch units in other continents, security has to be improved.

Bibliography

The United States became the world's largest LNG exporter in the first half of 2022. Homepage - U.S. Energy Information Administration (EIA). (n.d.). Retrieved November 30, 2022, from https://www.eia.gov/todayinenergy/detail.php?id=53159

Wikimedia Foundation. (2022, November 19). 2022 Nord Stream Gas Leaks. Wikipedia. Retrieved November 30, 2022, from https://en.wikipedia.org/wiki/2022_Nord_Stream_gas_leaks

Chevron Corporation, “liquefied natural gas (LNG): safely and efficiently transporting natural gas.” Accessed March 16, 2018. https://www.chevron.com/stories/liquefied-natural-gas

Energy.gov, “Liquefied Natural Gas (LNG).” Accessed March 16, 2018. https://energy.gov/fe/science-innovation/oil-gas/liquefied-natural-gas.

Shell Global, “Liquefied Natural Gas (LNG).” Accessed March 16, 2018. http://www.shell.com/energy-and-innovation/natural-gas/liquefied-natural-gas-lng.html.

Risk Assessment of Surface Transport of Liquid Natural Gas Cambridge Systematics, Inc.

"Guidelines for the safe transportation of liquefied natural gas (LNG) by road" by the International Association of Oil & Gas Producers (IOGP)

"LNG Cyber Security: A Survey of Cyber Risks and Mitigation Strategies for the LNG Industry" by the American Petroleum Institute (API)

"Liquefied Natural Gas (LNG) Supply Chain Security: An Overview" by the Congressional Research Service (CRS)

"LNG Transportation Security: A Comparative Analysis of Key Regulations and Standards" by the International Atomic Energy Agency (IAEA)

"Liquefied Natural Gas (LNG) Transportation Security: Background and Policy Options" by the Congressional Research Service (CRS)

Tang, Y., J. Jing, Z. Zhang, and Y. Yang. “A Quantitative Risk Analysis Method for the High Hazard Mechanical System in Petroleum and Petrochemical Industry,” Energies 11(1) (December 2017):14.

Appendix

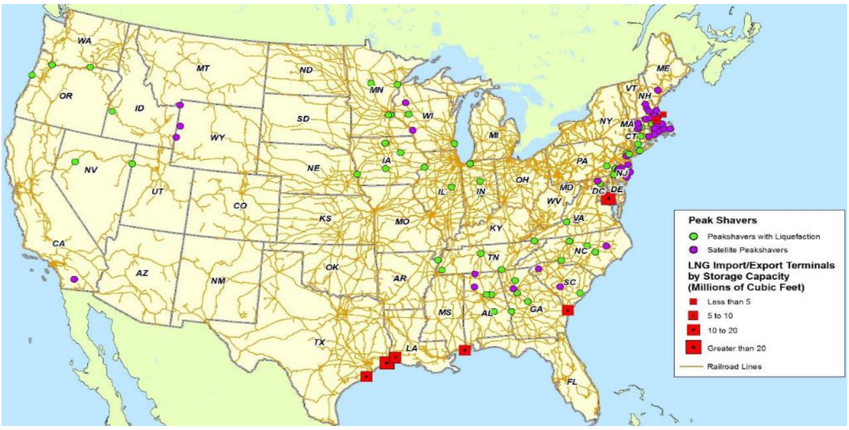
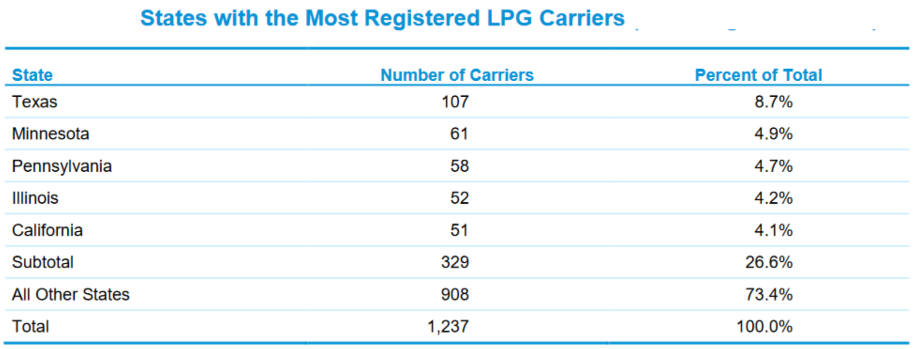


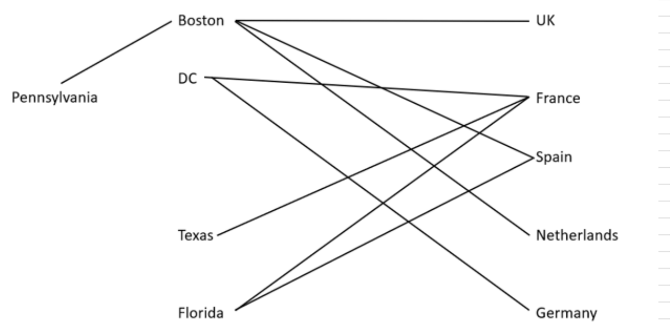
Figure 1.1 – Network Map in USA

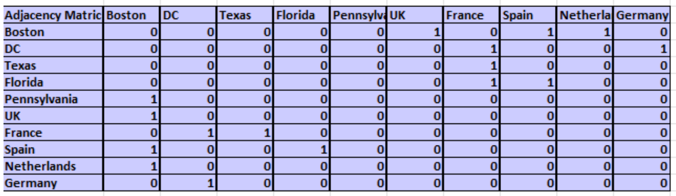


States with the Most Registered LPG Carriers

State	Number of Carriers	Percent of Total
Texas	107	8.7%
Minnesota	61	4.9%
Pennsylvania	58	4.7%
Illinois	52	4.2%
California	51	4.1%
Subtotal	329	26.6%
All Other States	908	73.4%
Total	1,237	100.0%

Figure 1.2 – Network Map in USA

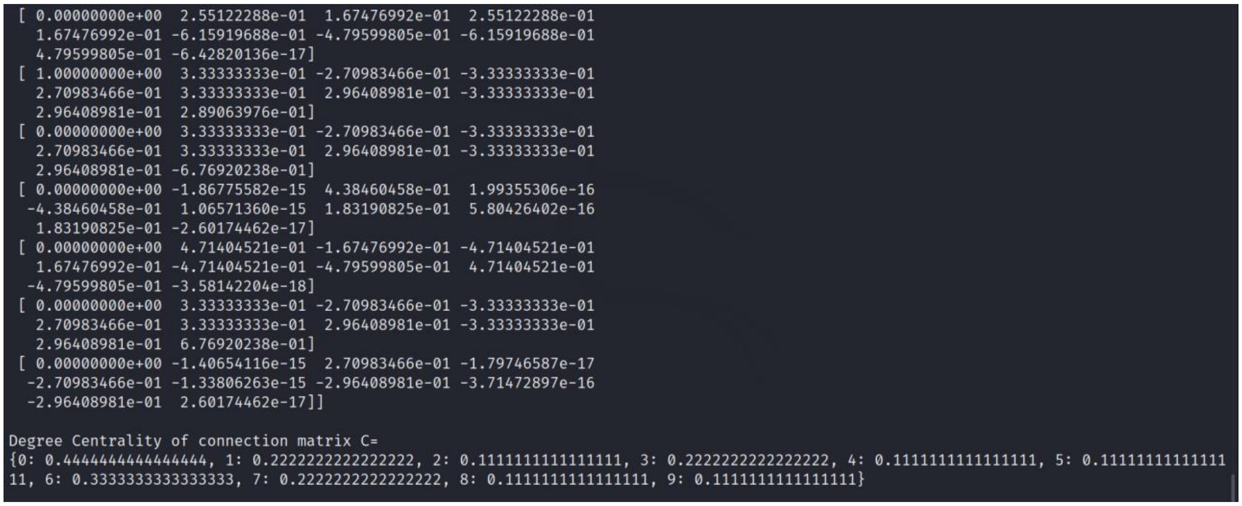




Adjacency Matric	Boston	DC	Texas	Florida	Pennsylva	UK	France	Spain	Netherla	Germany
Boston	0	0	0	0	0	1	0	1	1	0
DC	0	0	0	0	0	0	1	0	0	1
Texas	0	0	0	0	0	0	1	0	0	0
Florida	0	0	0	0	0	0	1	1	0	0
Pennsylvania	1	0	0	0	0	0	0	0	0	0
UK	1	0	0	0	0	0	0	0	0	0
France	0	1	1	0	0	0	0	0	0	0
Spain	1	0	0	1	0	0	0	0	0	0
Netherlands	1	0	0	0	0	0	0	0	0	0
Germany	0	1	0	0	0	0	0	0	0	0

```
[[0 0 0 0 0 1 0 1 1 0]
 [0 0 0 0 0 0 1 0 0 1]
 [0 0 0 0 0 0 1 0 0 0]
 [0 0 0 0 0 0 1 1 0 0]
 [1 0 0 0 0 0 0 0 0 0]
 [1 0 0 0 0 0 0 0 0 0]
 [0 1 1 0 0 0 0 0 0 0]
 [1 0 0 1 0 0 0 0 0 0]
 [1 0 0 0 0 0 0 0 0 0]
 [0 1 0 0 0 0 0 0 0 0]]
```

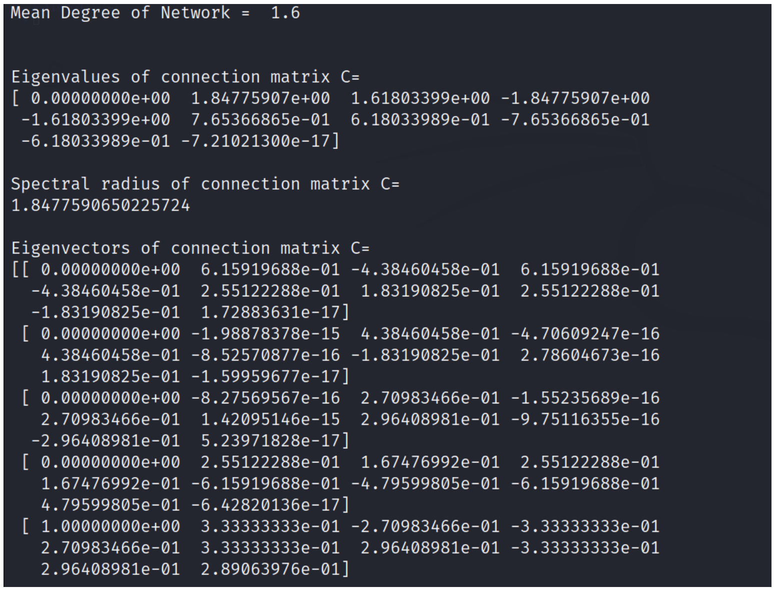
Figure 1.2 – Node, Link Network and Adjacency Matrix



```
 [ 0.00000000e+00  2.55122288e-01  1.67476992e-01  2.55122288e-01
   1.67476992e-01 -6.15919688e-01 -4.79599805e-01 -6.15919688e-01
   4.79599805e-01 -6.42820136e-17]
 [ 1.00000000e+00  3.33333333e-01 -2.70983466e-01 -3.33333333e-01
   2.70983466e-01  3.33333333e-01  2.96408981e-01 -3.33333333e-01
   2.96408981e-01  2.89063976e-01]
 [ 0.00000000e+00  3.33333333e-01 -2.70983466e-01 -3.33333333e-01
   2.70983466e-01  3.33333333e-01  2.96408981e-01 -3.33333333e-01
   2.96408981e-01 -6.76920238e-01]
 [ 0.00000000e+00 -1.86775582e-15  4.38460458e-01  1.99355306e-16
  -4.38460458e-01  1.06571360e-15  1.83190825e-01  5.80426402e-16
   1.83190825e-01 -2.60174462e-17]
 [ 0.00000000e+00  4.71404521e-01 -1.67476992e-01 -4.71404521e-01
   1.67476992e-01 -4.71404521e-01 -4.79599805e-01  4.71404521e-01
  -4.79599805e-01 -3.58142204e-18]
 [ 0.00000000e+00  3.33333333e-01 -2.70983466e-01 -3.33333333e-01
   2.70983466e-01  3.33333333e-01  2.96408981e-01 -3.33333333e-01
   2.96408981e-01  6.76920238e-01]
 [ 0.00000000e+00 -1.40654116e-15  2.70983466e-01 -1.79746587e-17
  -2.70983466e-01 -1.33806263e-15 -2.96408981e-01 -3.71472897e-16
  -2.96408981e-01  2.60174462e-17]]

Degree Centrality of connection matrix C=
{0: 0.4444444444444444, 1: 0.2222222222222222, 2: 0.1111111111111111, 3: 0.2222222222222222, 4: 0.1111111111111111, 5: 0.11111111111111
11, 6: 0.3333333333333333, 7: 0.2222222222222222, 8: 0.1111111111111111, 9: 0.1111111111111111}
```

Figure 1.3.1 – Python Script Results



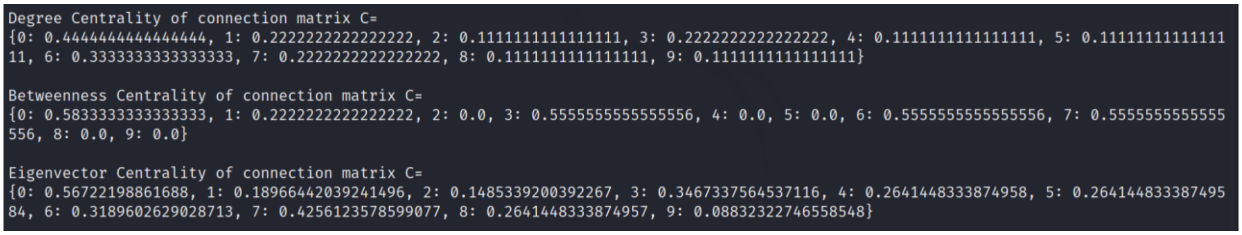
```
Mean Degree of Network =  1.6


Eigenvalues of connection matrix C=
[ 0.00000000e+00  1.84775907e+00  1.61803399e+00 -1.84775907e+00
 -1.61803399e+00  7.65366865e-01  6.18033989e-01 -7.65366865e-01
 -6.18033989e-01 -7.21021300e-17]

Spectral radius of connection matrix C=
1.8477590650225724

Eigenvectors of connection matrix C=
[[ 0.00000000e+00  6.15919688e-01 -4.38460458e-01  6.15919688e-01
  -4.38460458e-01  2.55122288e-01  1.83190825e-01  2.55122288e-01
  -1.83190825e-01  1.72883631e-17]
 [ 0.00000000e+00 -1.98878378e-15  4.38460458e-01 -4.70609247e-16
   4.38460458e-01 -8.52570877e-16 -1.83190825e-01  2.78604673e-16
   1.83190825e-01 -1.59959677e-17]
 [ 0.00000000e+00 -8.27569567e-16  2.70983466e-01 -1.55235689e-16
   2.70983466e-01  1.42095146e-15  2.96408981e-01 -9.75116355e-16
  -2.96408981e-01  5.23971828e-17]
 [ 0.00000000e+00  2.55122288e-01  1.67476992e-01  2.55122288e-01
   1.67476992e-01 -6.15919688e-01 -4.79599805e-01 -6.15919688e-01
   4.79599805e-01 -6.42820136e-17]
 [ 1.00000000e+00  3.33333333e-01 -2.70983466e-01 -3.33333333e-01
   2.70983466e-01  3.33333333e-01  2.96408981e-01 -3.33333333e-01
   2.96408981e-01  2.89063976e-01]
```

Figure 1.3.2 – Python Script Results



```
Degree Centrality of connection matrix C=
{0: 0.4444444444444444, 1: 0.2222222222222222, 2: 0.1111111111111111, 3: 0.2222222222222222, 4: 0.1111111111111111, 5: 0.11111111111111
11, 6: 0.3333333333333333, 7: 0.2222222222222222, 8: 0.1111111111111111, 9: 0.1111111111111111}

Betweenness Centrality of connection matrix C=
{0: 0.5833333333333333, 1: 0.2222222222222222, 2: 0.0, 3: 0.5555555555555556, 4: 0.0, 5: 0.0, 6: 0.5555555555555556, 7: 0.5555555555555
556, 8: 0.0, 9: 0.0}

Eigenvector Centrality of connection matrix C=
{0: 0.56722198861688, 1: 0.18966442039241496, 2: 0.1485339200392267, 3: 0.3467337564537116, 4: 0.2641448333874958, 5: 0.264144833387495
84, 6: 0.3189602629028713, 7: 0.4256123578599077, 8: 0.2641448333874957, 9: 0.08832322746558548}
```

Figure 1.3.3 – Python Script Results

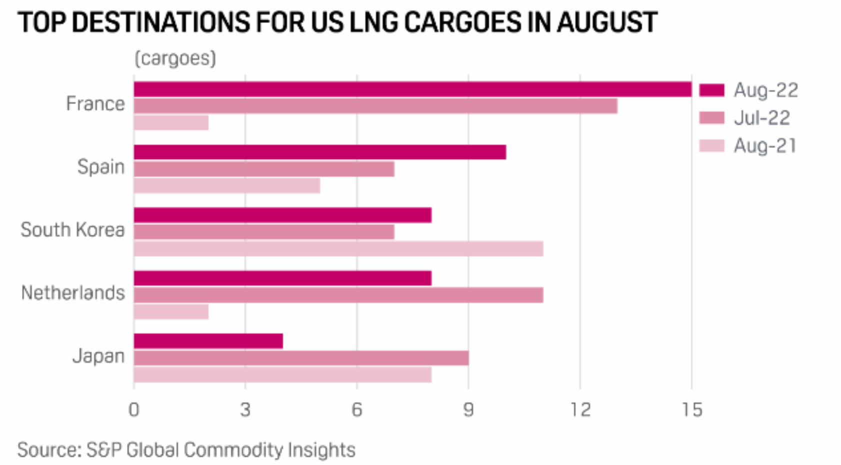
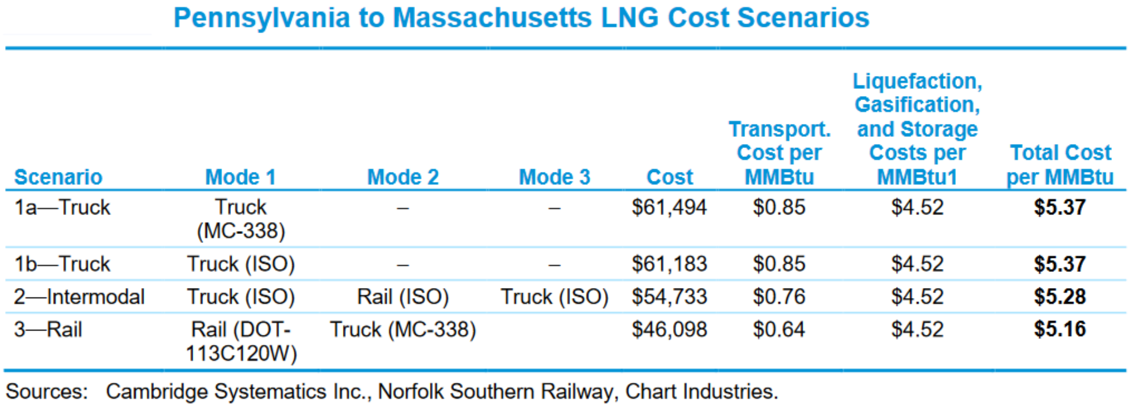


Figure 1.4 – LNG Exports by USA (Top 5)



Pennsylvania to Massachusetts LNG Cost Scenarios

Scenario	Mode 1	Mode 2	Mode 3	Cost	Transport. Cost per MMBtu	Liquefaction, Gasification, and Storage Costs per MMBtu1	Total Cost per MMBtu
1a—Truck	Truck (MC-338)	–	–	$61,494	$0.85	$4.52	**$5.37**
1b—Truck	Truck (ISO)	–	–	$61,183	$0.85	$4.52	**$5.37**
2—Intermodal	Truck (ISO)	Rail (ISO)	Truck (ISO)	$54,733	$0.76	$4.52	**$5.28**
3—Rail	Rail (DOT-113C120W)	Truck (MC-338)		$46,098	$0.64	$4.52	**$5.16**

Sources: Cambridge Systematics Inc., Norfolk Southern Railway, Chart Industries.

Figure 1.5 – LNG Costs by Road – Pennsylvania to Massachusetts

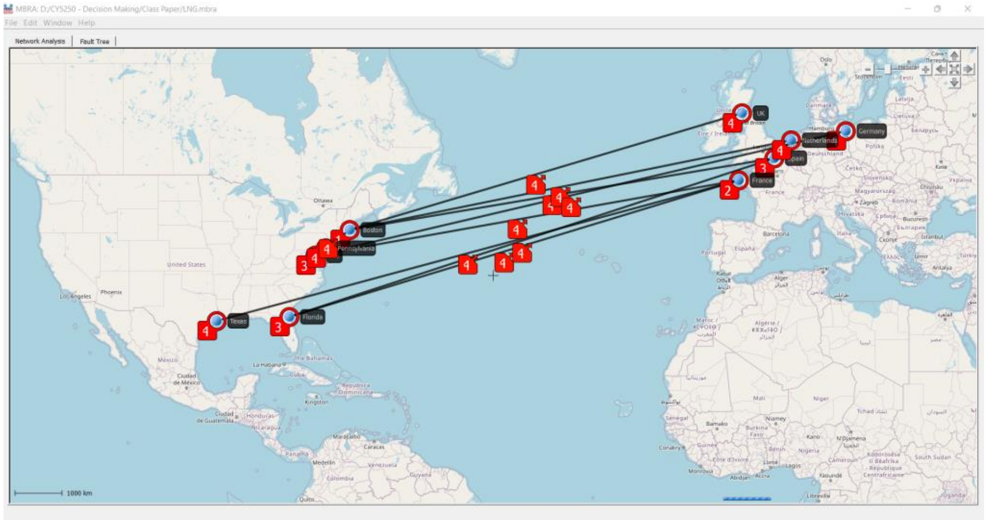
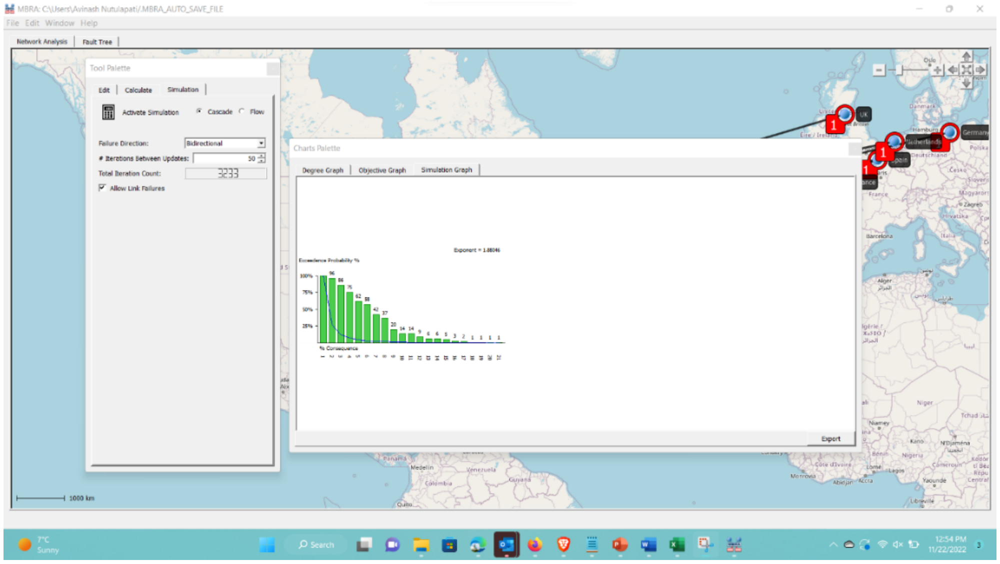


Figure 1.6 – MBRA


MBRA: C:\Users\Avinash Nutulapati/.MBRA_AUTO_SAVE_FILE

Tool Palette — Edit | Calculate | Simulation

Activate Simulation ● Cascade ○ Flow

Failure Direction: Bidirectional

# Iterations Between Updates: 50

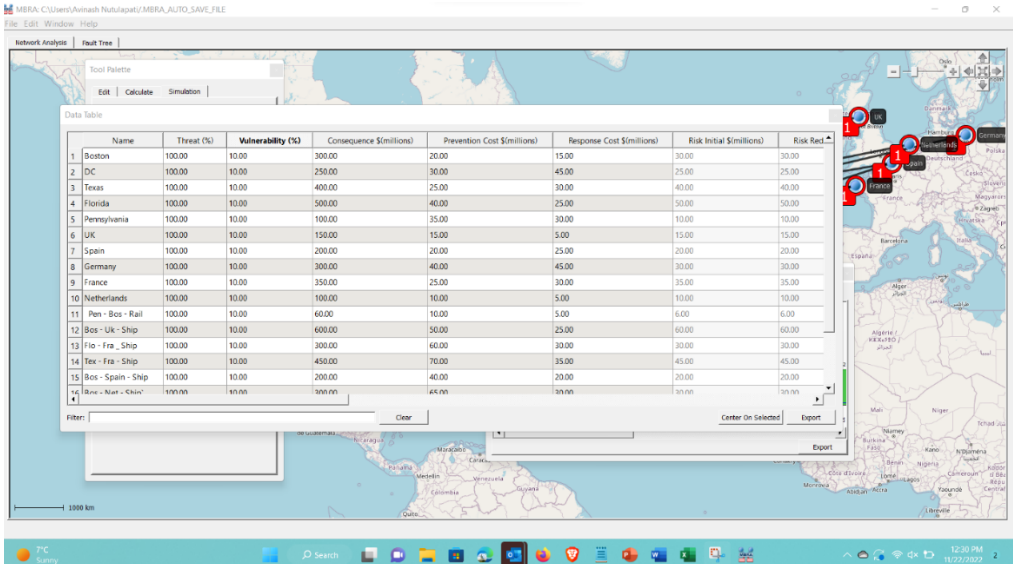
Total Iteration Count: 3233

☑ Allow Link Failures

Charts Palette — Degree Graph | Objective Graph | Simulation Graph

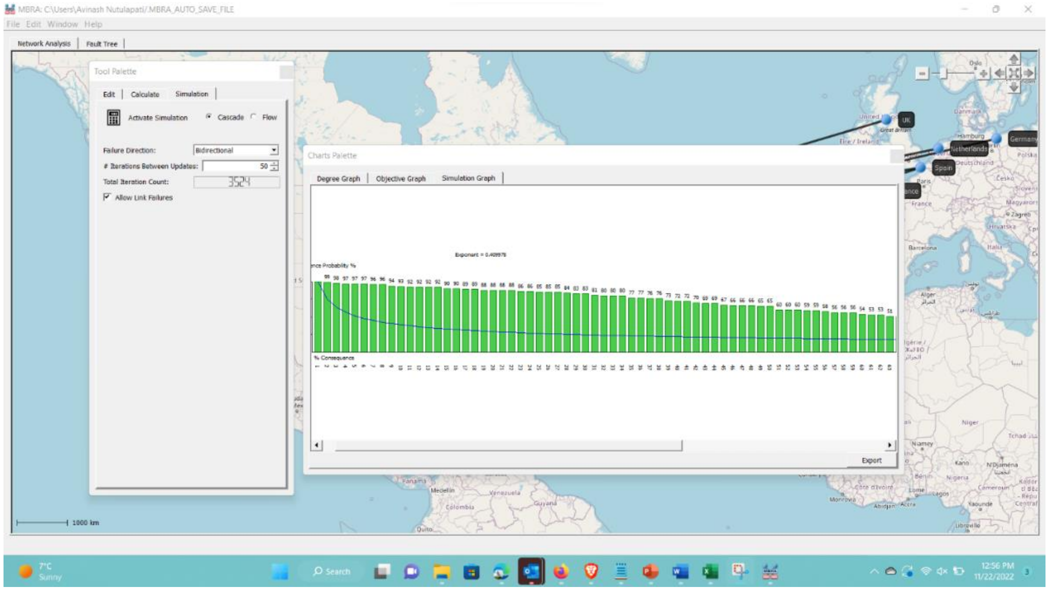
Exponent = 1.88046

Figure 1.6.1 – Simulation Graph : Vulnerability:10%, Q1=1.8



	Name	Threat (%)	**Vulnerability (%)**	Consequence $(millions)	Prevention Cost $(millions)	Response Cost $(millions)	Risk Initial $(millions)	Risk Red
1	Boston	100.00	10.00	300.00	20.00	15.00	30.00	30.00
2	DC	100.00	10.00	250.00	30.00	45.00	25.00	25.00
3	Texas	100.00	10.00	400.00	25.00	30.00	40.00	40.00
4	Florida	100.00	10.00	500.00	40.00	25.00	50.00	50.00
5	Pennsylvania	100.00	10.00	100.00	35.00	30.00	10.00	10.00
6	UK	100.00	10.00	150.00	15.00	5.00	15.00	15.00
7	Spain	100.00	10.00	200.00	20.00	25.00	20.00	20.00
8	Germany	100.00	10.00	300.00	40.00	45.00	30.00	30.00
9	France	100.00	10.00	350.00	25.00	30.00	35.00	35.00
10	Netherlands	100.00	10.00	100.00	10.00	5.00	10.00	10.00
11	Pen - Bos - Rail	100.00	10.00	60.00	10.00	5.00	6.00	6.00
12	Bos - Uk - Ship	100.00	10.00	600.00	50.00	25.00	60.00	60.00
13	Flo - Fra _ Ship	100.00	10.00	300.00	60.00	30.00	30.00	30.00
14	Tex - Fra - Ship	100.00	10.00	450.00	70.00	35.00	45.00	45.00
15	Bos - Spain - Ship	100.00	10.00	200.00	40.00	20.00	20.00	20.00
16	Bos - Net - Ship'	100.00	10.00	300.00	65.00	30.00	30.00	30.00

Figure 1.6.1.1 – Data Table : Vulnerability:10%



Activate Simulation ● Cascade ○ Flow

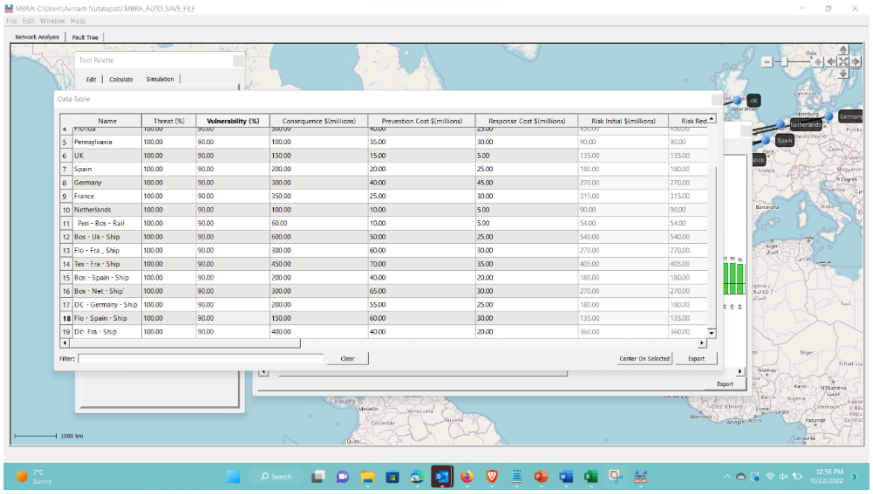
Failure Direction: Bidirectional

Iterations Between Updates: 50

Total Iteration Count: 3524

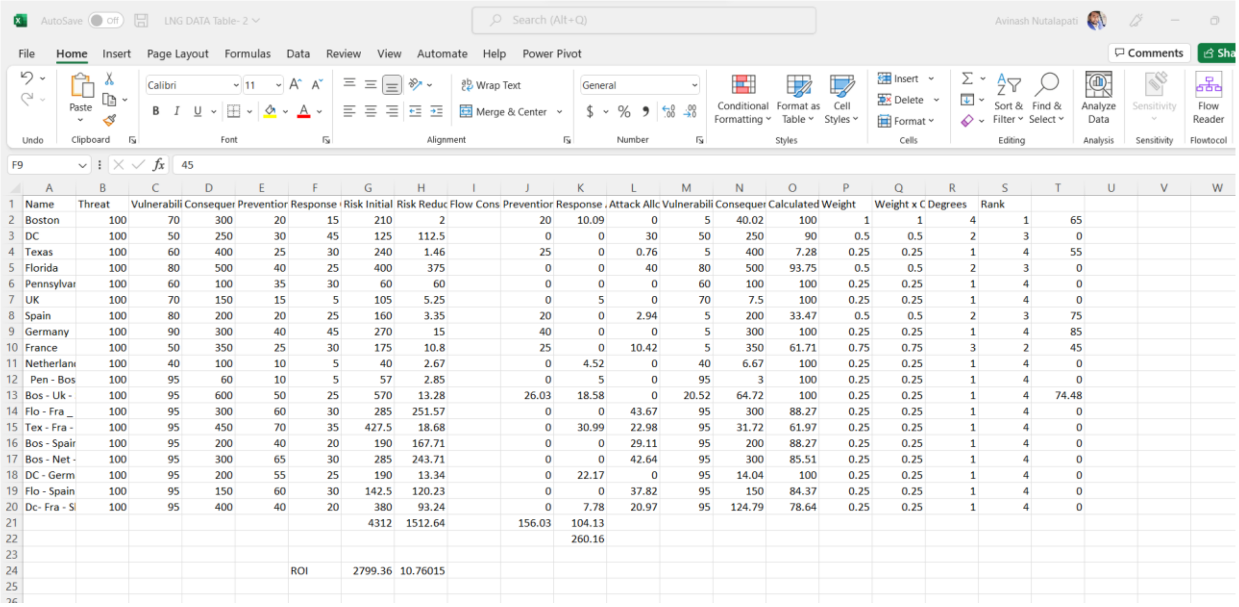
☑ Allow Link Failures

Figure 1.6.2 – Simulation Graph : Vulnerability:90%, Q2=0.4



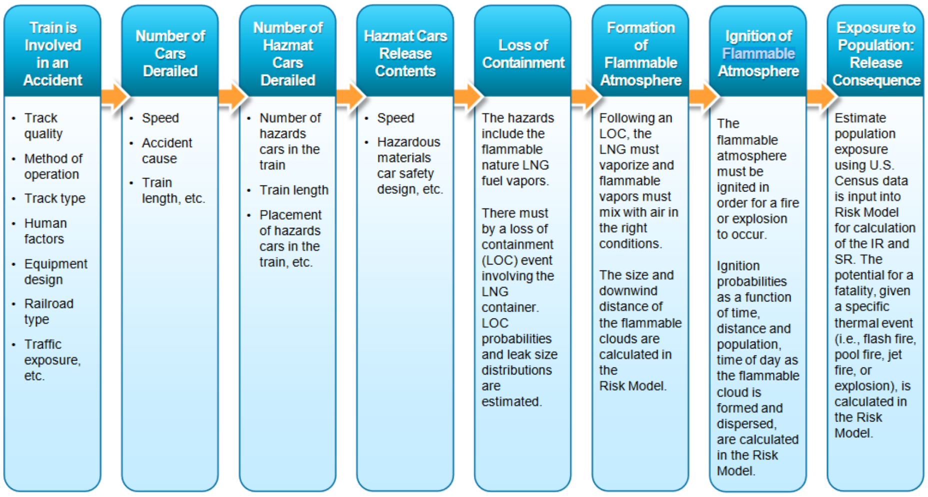
	Name	Threat (%)	Vulnerability (%)	Consequence $(millions)	Prevention Cost $(millions)	Response Cost $(millions)	Risk Initial $(millions)	Risk Red.
4	Florida	100.00	90.00	500.00	40.00	25.00	450.00	450.00
5	Pennsylvania	100.00	90.00	100.00	35.00	30.00	90.00	90.00
6	UK	100.00	90.00	150.00	15.00	5.00	135.00	135.00
7	Spain	100.00	90.00	200.00	20.00	25.00	180.00	180.00
8	Germany	100.00	90.00	300.00	40.00	45.00	270.00	270.00
9	France	100.00	90.00	350.00	25.00	30.00	315.00	315.00
10	Netherlands	100.00	90.00	100.00	10.00	5.00	90.00	90.00
11	Pen - Bos - Rail	100.00	90.00	60.00	10.00	5.00	54.00	54.00
12	Bos - Uk - Ship	100.00	90.00	600.00	50.00	25.00	540.00	540.00
13	Flo - Fra _ Ship	100.00	90.00	300.00	60.00	30.00	270.00	270.00
14	Tex - Fra - Ship	100.00	90.00	450.00	70.00	35.00	405.00	405.00
15	Bos - Spain - Ship	100.00	90.00	200.00	40.00	20.00	180.00	180.00
16	Bos - Net - Ship`	100.00	90.00	300.00	65.00	30.00	270.00	270.00
17	DC - Germany - Ship	100.00	90.00	200.00	55.00	25.00	180.00	180.00
18	Flo - Spain - Ship	100.00	90.00	150.00	60.00	30.00	135.00	135.00
19	Dc- Fra - Ship	100.00	90.00	400.00	40.00	20.00	360.00	360.00

Figure 1.6.2.1 – Data Table: Vulnerability:90%



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	Name	Threat	Vulnerabili	Consequer	Preventior	Response (	Risk Initial	Risk Reduc	Flow Cons	Preventior	Response .	Attack Allc	Vulnerabili	Consequer	Calculated	Weight	Weight x C	Degrees	Rank	
2	Boston	100	70	300	20	15	210	2		20	10.09	0	5	40.02	100	1	1	4	1	65
3	DC	100	50	250	30	45	125	112.5		0	0	30	50	250	90	0.5	0.5	2	3	0
4	Texas	100	60	400	25	30	240	1.46		25	0	0.76	5	400	7.28	0.25	0.25	1	4	55
5	Florida	100	80	500	40	25	400	375		0	0	40	80	500	93.75	0.5	0.5	2	3	0
6	Pennsylvar	100	60	100	35	30	60	60		0	0	0	60	100	100	0.25	0.25	1	4	0
7	UK	100	70	150	15	5	105	5.25		0	5	0	70	7.5	100	0.25	0.25	1	4	0
8	Spain	100	80	200	20	25	160	3.35		20	0	2.94	5	200	33.47	0.5	0.5	2	3	75
9	Germany	100	90	300	40	45	270	15		40	0	0	5	300	100	0.25	0.25	1	4	85
10	France	100	50	350	25	30	175	10.8		25	0	10.42	5	350	61.71	0.75	0.75	3	2	45
11	Netherlan	100	40	100	10	5	40	2.67		0	4.52	0	40	6.67	100	0.25	0.25	1	4	0
12	Pen - Bos	100	95	60	10	5	57	2.85		0	5	0	95	3	100	0.25	0.25	1	4	0
13	Bos - Uk -	100	95	600	50	25	570	13.28		26.03	18.58	0	20.52	64.72	100	0.25	0.25	1	4	74.48
14	Flo - Fra _	100	95	300	60	30	285	251.57		0	0	43.67	95	300	88.27	0.25	0.25	1	4	0
15	Tex - Fra -	100	95	450	70	35	427.5	18.68		0	30.99	22.98	95	31.72	61.97	0.25	0.25	1	4	0
16	Bos - Spair	100	95	200	40	20	190	167.71		0	0	29.11	95	200	88.27	0.25	0.25	1	4	0
17	Bos - Net -	100	95	300	65	30	285	243.71		0	0	42.64	95	300	85.51	0.25	0.25	1	4	0
18	DC - Germ	100	95	200	55	25	190	13.34		0	22.17	0	95	14.04	100	0.25	0.25	1	4	0
19	Flo - Spain	100	95	150	60	30	142.5	120.23		0	0	37.82	95	150	84.37	0.25	0.25	1	4	0
20	Dc- Fra - Sl	100	95	400	40	20	380	93.24		0	7.78	20.97	95	124.79	78.64	0.25	0.25	1	4	0
21							4312	1512.64		156.03	104.13									
22											260.16									
23																				
24						ROI	2799.36	10.76015												
25																				

Figure 1.7 – ROI Calculation



Train is Involved in an Accident

- Track quality
- Method of operation
- Track type
- Human factors
- Equipment design
- Railroad type
- Traffic exposure, etc.

Number of Cars Derailed

- Speed
- Accident cause
- Train length, etc.

Number of Hazmat Cars Derailed

- Number of hazards cars in the train
- Train length
- Placement of hazards cars in the train, etc.

Hazmat Cars Release Contents

- Speed
- Hazardous materials car safety design, etc.

Loss of Containment

The hazards include the flammable nature LNG fuel vapors.

There must by a loss of containment (LOC) event involving the LNG container. LOC probabilities and leak size distributions are estimated.

Formation of Flammable Atmosphere

Following an LOC, the LNG must vaporize and flammable vapors must mix with air in the right conditions.

The size and downwind distance of the flammable clouds are calculated in the Risk Model.

Ignition of Flammable Atmosphere

The flammable atmosphere must be ignited in order for a fire or explosion to occur.

Ignition probabilities as a function of time, distance and population, time of day as the flammable cloud is formed and dispersed, are calculated in the Risk Model.

Exposure to Population: Release Consequence

Estimate population exposure using U.S. Census data is input into Risk Model for calculation of the IR and SR. The potential for a fatality, given a specific thermal event (i.e., flash fire, pool fire, jet fire, or explosion), is calculated in the Risk Model.

Figure 1.8 – Threats of LNG

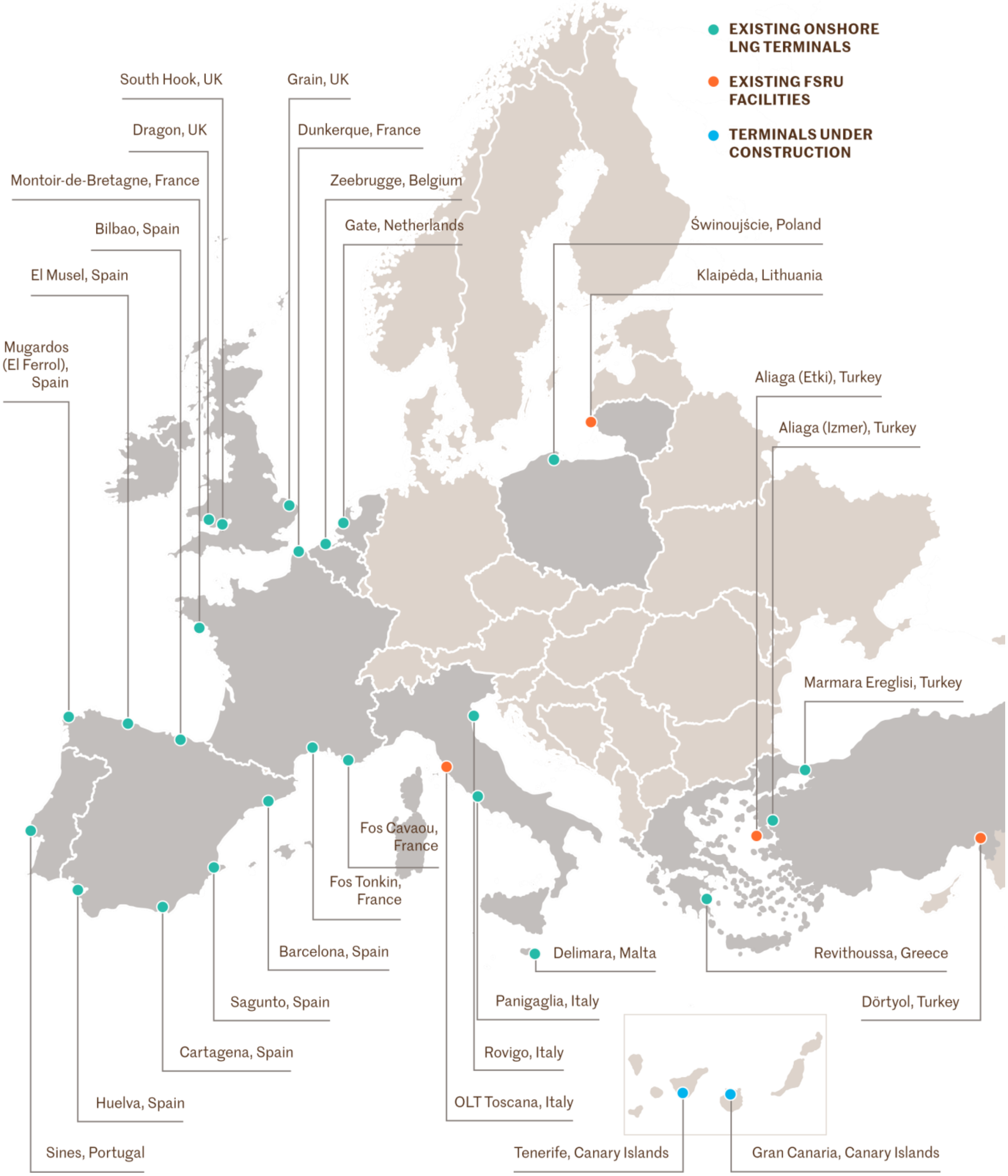
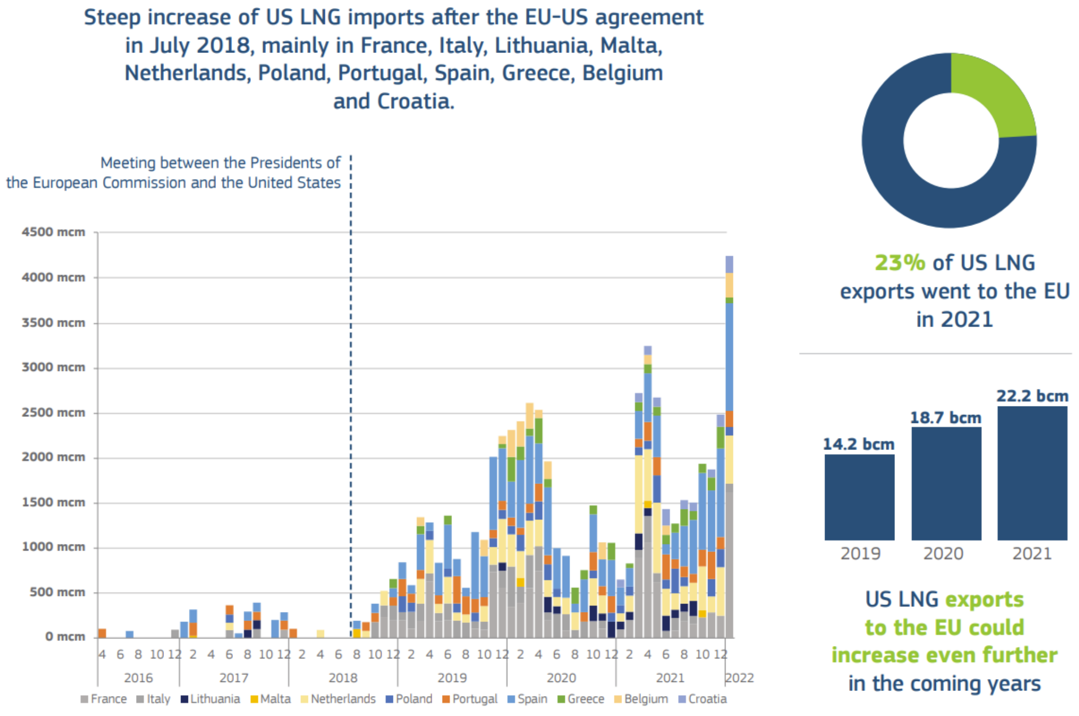
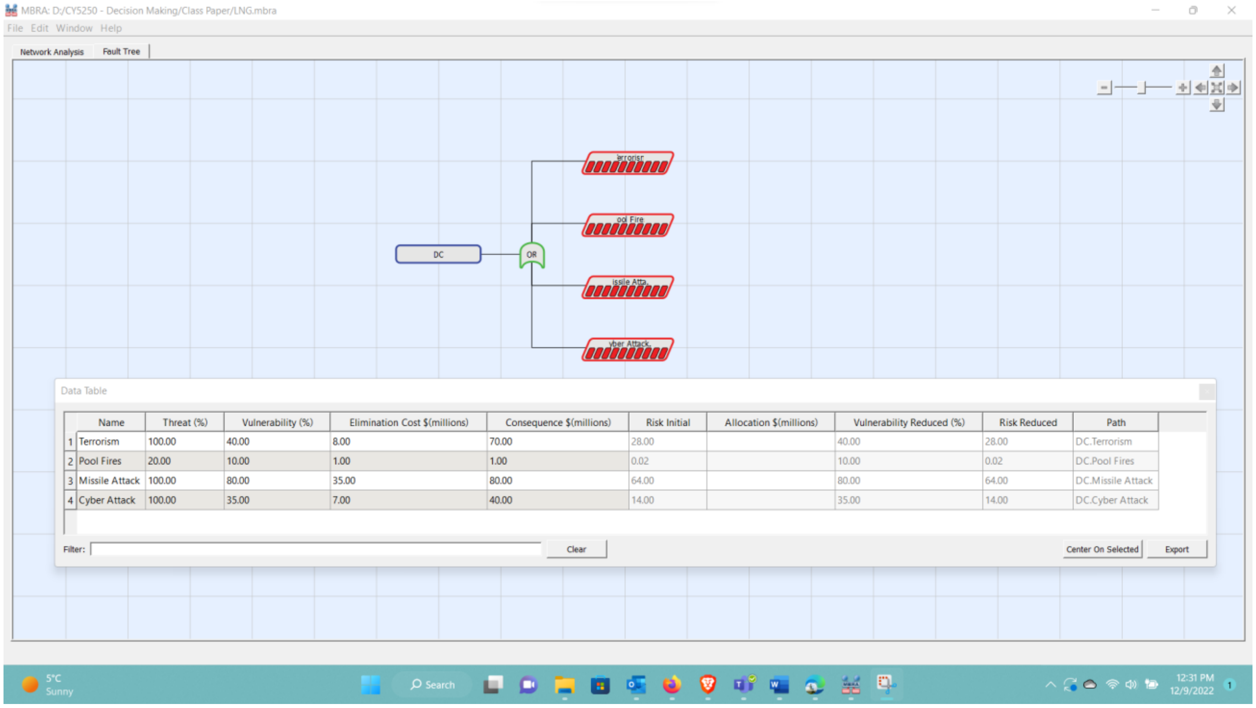


Figure 1.9 – LNG Import facilities in Europe



* *Data until 2 February 2022*
Source: European Commission.

Figure 1.10 – US LNG exports to Europe (Bu no. of units) – Graph



	Name	Threat (%)	Vulnerability (%)	Elimination Cost $(millions)	Consequence $(millions)	Risk Initial	Allocation $(millions)	Vulnerability Reduced (%)	Risk Reduced	Path
1	Terrorism	100.00	40.00	8.00	70.00	28.00		40.00	28.00	DC.Terrorism
2	Pool Fires	20.00	10.00	1.00	1.00	0.02		10.00	0.02	DC.Pool Fires
3	Missile Attack	100.00	80.00	35.00	80.00	64.00		80.00	64.00	DC.Missile Attack
4	Cyber Attack	100.00	35.00	7.00	40.00	14.00		35.00	14.00	DC.Cyber Attack

Figure 1.11 – FTA (fault Tree Analysis)