Guidebook: Principles and Best Practices for Supply Chain Resiliency1

Project Summary

A salient lesson from COVID-19 is the fragility of our supply chain caused by myriad types of disrupting events. These disrupting events may be natural (e.g., weather-related such as hurricanes), fabricated (e.g., accidents, cyber-attacks, transportation failures), or other (e.g., pandemics, geopolitical instability). The most recent supply chain disruptions caused severe consequences to the economic and national security resulting in increased prices, these disrupting events differ in their causes and provenance. Regardless of their causes and provenance, the disrupting events result in common consequences responsible for disrupting the supply chain including unacceptable delays, bottlenecks, and compromised operations with cascading consequences through both maritime and inter- modal transportation systems. These supply chain consequences pose significant risk to maritime transportation systems (MTS).

This project examined these disrupting events and their impact to design a set of resiliency principles and best practices for maritime supply chains from the viewpoint of vessel management as executed by the United States Coast Guard (USCG). Beyond the initial use of these best practices and guidelines for the Department of Homeland Security (DHS) and the USCG, there has been considerable interest in the TAMU-Galveston's network of Industry Board Advisors that these findings might be useful to those involved in commercial shipping. Unarguably, commercial shipping has a different mission than the Coast Guard, however, each entity will benefit if the principles and best practices are integrated and transparent, giving each insight into the other entity.

Project Goal: The project goal is to derive resiliency principles and best practices for the maritime supply chain economy applicable to both the operational (OT) and information (IT) technologies environment to establish the basis to develop our next generation, resilient data-driven supply chain network. As well, the project will identify gaps and voids in resiliency concepts for the basis of further research and technology development.

[1] Funded by through United States Department of Homeland Security under Grant Award Number 18STCBT00001 through the United States Department of Homeland Center of Excellence at Texas A&M University, the Cross-Border Threat Screening and Supply Chain Defense (CBTS).

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Project Innovations: The innovations in this project include the development of a supply chain maturity model and associated metrics. Previous supply chain maturity models are from the viewpoint of those who have custody and control of the goods and cargo in the supply chain. Further, their profitability depends on the efficient movement of these goods and cargo so their decisions may be optimized for the respective entity and not over a larger group of entities. Because supplies chains are so complex, the dependencies between factors affecting supply chains are also more complicated. When one aspect of the supply chain is compromised by a disrupting event, it cascades throughout the supply chain causing further disruptions. For example, when the Ever Given obstructed the Suez Canal in 2021, there were nearly 150 ships queued behind the Ever Given. Many had contractual issues for delivery of goods. Others may have had cargo that would expire if not delivered on time. Each of these disruptions causes further disruptions for those who needed these good delivered on time that would, in turn, case disruptions in their respective entities as well as affect their countries. Ships could forego this route, but take on a longer voyage and added risk due to increased costs as well as piracy by traveling around the African continent. Typically, dependencies are modeled, often using Bayesian statistics, to determine the unintended consequences.

The dependencies would have an economic impact on the supply chain, and the responsibility, responsiveness, and overall interaction of the Coast Guard can be of major importance for mitigating the consequences of the supply chain downfall caused by the disrupting events. The innovation in this project is developing the supply chain maturity model for a more holistic model of the more complex dependencies comprising the supply chain and expanding the viewpoints to include those who manage vessel traffic without having custody or control of the goods and cargo within the physical supply chain.

The second innovation are metrics that derive the supply chain maturity. These metrics are those near-real-time measurable factors that can be used to better manage vessel traffic. Further the understanding of these metrics – their capture, storage, and further data analysis – can be used to implement industry best practices to increase the level of the maturity in the model for the organization.

Project Scope: The scope of this guidebook is to provide guidelines for building resiliency in the supply chain from a vessel traffic management viewpoint. There are three types of flows in any supply chains: *the physical flow* of materials and goods often managed by logistics systems, *the electronic flow of information*, and *the physical or electronic flow of currency.* The scope of this project is the second relative to the first, or more precisely the electronic flow of information regarding the physical flow of materials and goods that the USCG uses to make its decisions based to manage vessel traffic.

Viewpoint: The viewpoint of this guidebook is the United States Coast Guard (USCG) as vessel traffic managers. There are a number of recognized supply chain disruptors[2], however this project recognizes only those within the purview of the USCG. For example, the USCG does not have jurisdiction over detecting counterfeit goods as that falls to its sister agency, Customs and Border Patrol in the Department of Homeland Security, nor do they have control over the actual sourcing, production, or product tampering that may occur during manufacturing. The viewpoint of the USCG begins where goods and cargo enter their jurisdiction from international waters into those waterways controlled by the United States. That is, when and where the goods and cargo enter the ocean or inland waterways – managed by the UCSG information technology (IT) systems until the goods and cargo exit waterways and enter inter-modal (i.e., trucks and rail) transportation. Hence, our project focuses on the data provided by the information flow governing supply chain to better manage the physical movement of vessels that is within the purview of the USCG.

Broader Impact: Although a key stakeholder in this project is the United States Coast Guard (USCG), the results are also useful to the commercial shipping industry who directly controls the goods and cargo in the supply chain. As such, we are requesting review of the research results from industry sources after review by the USCG and DHS.

Project Deliverable: This report documents the research results to date and includes the principles and best practices for resiliency in the supply chain as well as an overview of the research.

[2] Examples of supply chain disruptors include counterfeit parts, malicious insiders, tampering, theft, insertion of malicious software or hardware, or loss of operations. **(Special Publication 800-161)** https://doi.org/10.6028/NIST.SP.800-161r1. Or [NIST SP 800-53 Rev. 5.

Summary of Principles and Best Practices: Technology, People, Processes

Supply chain resiliency is the ability to anticipate, withstand, recover from, and adapt to disrupting events within the supply chain. Optimally, resilient systems are resilient from their initial design, however, systems must be adapted to provide resiliency. Further, given (1) the dynamic nature of new technologies implemented with legacy systems and (2) the dynamic maritime transportation environment, the goal of resiliency is a moving target. As such, there must be a continuous focus on the principles and best practices associated with building resiliency into the supply chain.

While there are many areas in which to build resiliency, due to the scope of the research effort, we have identified five areas in this phase of the research to improve the supply chain resiliency. These are based on NIST SP 800-53 R5 controls that are utilized throughout the NIST supply chain work. [3]

I. **Awareness and Training (AT)** includes (i) awareness programs which set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure; (ii) training which teaches people the skills that will enable them to perform their jobs more effectively; and (iii) education which is targeted for security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities.

II. **Physical Environment (PE)** whereby organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

III. **Provenance** which includes the records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to appropriate actors, functions, locales, or activities.[4]

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

[4] https://csrc.nist.gov/glossary/term/provenance

IV. **Risk Management (RM)** is the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.[5]

V. **Incident Response (IR)** is the mitigation of violations of security policies and recommended practices.[6] IR has become more important as experience shows we cannot prevent the incidents and need to be better prepared to respond.

The following is a summary of the overarching principles and associated best practices with resiliency in the supply chain followed by explanatory discussion on the background of these principles.

[5] https://csrc.nist.gov/glossary/term/risk_management

[6] https://csrc.nist.gov/glossary/term/incident_response

Technology

Principle T-1: Recognize that effective supply chain and vessel management relies on extensive, near real-time data. The level of this data is under the purview and control of the USCG, and as such, it is reliable and available. (High Priority)

Most Closely Related to Risk Management and Incident Response

Product: Summary of available USCG data sources with their specific data focus and content.

I. **Best Practice T1-1:** Maintain a central repository of available USCG sources[7,8] including the Marine Information for Safety and Law enforcement (MISLE)[9].

II. **Best Practice T1-2:** Utilize the data sources as available related to vessel management and supply chain.

III. **Best Practice T1-3**: Periodically review and update the USCG data and IT systems and check for data duplication.

IV. **Best Practice T1-4**: Maintain visibility into the periodic reviews and updates on the USCG data and IT systems. Assign one team member to maintain information on these systems.

V. **Best Practice T1-5**: Prepare and maintain key data development process for maintaining data reliability.

VI. **Best Practice T1-6**: Maintain and manage reliable data through the integrated data environment (Logistics information management system).

VII. **Best Practice T1-7**: Provide training to the responsible data maintenance teams for maintaining error- free data systems.

VIII. **Best Practice T1-8:** Prepare a summary of all the available USCG data related to supply chain and Vessel management, information about relevant systems to be included and mention from where data was retrieved.

IX. **Best Practice T1-9:** Prepare a designated data team responsible for extracting reliable data from various USCG platforms along with the relevant departments, for providing immediate assistance with disruptive events.

Possible Best Practice Enhancements/Future Research: Consider interoperability with other non-government data sources. This may already be done but is not documented on any USCG source.

[7] https://cg.portal.uscg.mil/units/OCDO/guidingdocuments/USCG-Data-Strategy_2021.02.03_Final.pdf

[8] https://www.mycg.uscg.mil/News/Article/2521127/coast-guards-first-data-strategy-guides-the-way-forward-for-data-readiness-and/

[9] https://www.dhs.gov/publication/dhsuscgpia-008-marine-information-safety-and-law-enforcement-misle#:~:text=The%20MISLE%20system%20is%20a,protection%20and%20law%20enforcement%20programs.

Principle T-2: Require technology interoperability. (High Priority)

Most Closely Related to Risk Management and Incident Response

Product: Technology Status Report and Plan of Actions and Milestones (POA&M)

I. Best Practice T2-1: Require that standard standards and protocols are used throughout the maritime environment including third party entities.

II. Best Practice T2-2: Conduct a gap analysis to determine the difference between what is required (To-Be) and what is being practiced (As-Is).

III. Best Practice T2-3: From the gap analysis, develop a Plan of Action & Milestones (POA&M) that will be reviewed periodically (no more than quarterly) for the resolving the issues.

IV. Best Practice T2-4: Conduct periodic audits to ensure that the standards and protocols are being used and up to date.

V. Best Practice T2-5: Prepare a summary of the required standards and protocols summarizing key components of each to be followed from USCG and third-party entities.

VI. Best Practice T2-6: Have a designated team to work with third parties for monitoring technology's status/ interoperability and if any update/correction is required.

Possible Best Practice Enhancements/Future Research:

Research interoperability with third party entities for designing modern technology standard and protocols for new emerging technologies for better usage understanding.

Principle T-3: Incorporate an innovation plan to exploit modern technologies (e.g., 5G, sensors, drones) to enable improved incident identification and response. (Medium Priority)

Most Closely Related to Risk Management and Incident Response

Product: Emerging Technologies Report

I. Best Practice T3-1: Prepare a detailed innovation/implementation plan explaining how these emerging technologies will assist USCG operations to identify and respond to incidents.

II. Best Practice T3-2: Prepare a detailed implementation plan listing all the modern technologies, their full characteristics and delineation.

III. Best Practice T3-3: Prepare training sessions for full familiarization of the new emerging technologies.

IV. Best Practice T3-4: Implement intervals for checking the efficacy of the modern technology.

V. Best Practice T1-5: Prepare milestone/action plan for evaluating the emerging technologies assistance in conjunction with the relevant departments/facilities and third parties for checking for improvements which will help incident identification.

Possible Best Practice Enhancements/Future Research:

Research mechanisms for considering how emerging technologies from third parties will impact operations. Consider preparing emerging technologies report with third parties and outline required training sessions and improvements.

People

Principle PE-1: Identify stakeholders to collaborate in the maritime environment. (Medium Priority)

Most Closely Related to Awareness and Training, Risk Management, Provenance, and Incident Response

Product: Stakeholder Lists, Contact List

I. **Best Practice PE1-1:** Identify and engage stakeholders both in maritime transportation systems and in the inter-modal transportation systems. Utilize public – private partnerships by integrating with industry and professional associations.

II. **Best Practice PE1-2:** Utilize existing mechanisms or create new mechanisms to communicate clearly the status of and provide visibility into the supply chain for the stakeholders.

III. **Best Practice PE1-3:** Designate a USCG individual to maintain a close relationship with DHS, DoD, Maritime Cyber Readiness Branch (MCRB), Cybersecurity and Infrastructure Security Agency (CISA), CGCYBER's Maritime Cyber Readiness Branch (MCRB) and provisioning of cyber resiliency assessments.

IV. **Best Practice PE1-4:** Maintain a training schedule for all levels of stakeholders. To determine the efficacy of the training, conduct periodic audits by holding table-top exercises for simulated scenarios or with spontaneous drills.

Possible Best Practice Enhancements/Future Research:

Consider the value of preparing and regularly updating a stakeholders contact list from the maritime and inter-modal transportation cluster, private or public would enhance communication. Include a brief explanation of their business description and potential assistance to specific disruptive events.

Processes

Principle PR-1: Assume incidents will occur and prepare accordingly by preparing a specific Risk Management Plan for the disrupting events focusing on the risks with the highest consequences (even if low priorities). (High Priority)

Most Closely Related to Risk Management and Incident Response

Products: Risk Management Assessment

I. **Best Practice PR1-1:** Prepare specific risk management assessment plan for high-risk disruptive events while focusing on geographical areas.

II. **Best Practice PR1-2:** Prepare clear updated risk management assessment policies for risks with highest consequences, aligned with the USCG goals and objectives.

III. **Best Practice PR1-3:** Contact periodic risk assessment meetings involving major USCG stakeholders for discussing immediate or predicted disrupting events with high consequences and update the risk management plan accordingly.

IV. **Best Practice PR1-4:** Have a designated risk team to be ready to follow up a risk assessment plan along with a mitigation plan for assuming incidents.

V. **Best Practice PR1-5:** Maintain a Program Actions & Milestone Plan of the gap analysis between what is planned and what is achieved for periodic review.

VI. **Best Practice T1-6**: Prepare a summary of high disruptive events and prepare period tests with third parties for helping the relevant parties to understand their role in these events.

Possible Best Practice Enhancements/Future Research:

Prepare in collaboration with third parties emergency response plans for high-risk events, which will include several geographical areas, and will explain how USCG authorization can contribute to the prevention and mitigation of a high disruptive event.

Principle PR-2: Assume incidents will occur and prepare accordingly by preparing an Incident Response Plan. (High Priority)

Most Closely Related to Risk Management and Incident Response

Products: Incident Response Plan

I. Best Practice PR2-1: Prepare for an incident by performing a Risk Assessment of potential incidents focusing on both the causes and the consequences of the incident.

II. Best Practice PR2-2: Based on the Risk Assessment, prepare for an incident by documenting an Incident Response plan.

III. Best Practice PR2-3: Prepare for an actual incident response by providing training/awareness and practicing simulated exercises.

IV. Best Practice PR2-4: Prepare for the long-term consequences of an incident by documenting and practicing a Contingency Plan with several scenarios depending on the timeline of the incident and the severity of the consequences
   a. Within the Contingency Plan, following IMO AND ISPS Codes is mandatory

V. Best Practice PR2-5: After an incident, hold a Lessons Learned meetings to improve on the Incident Response Plan by planning on incorporating those lessons learned.

Possible Best Practice Enhancements/Future Research:

Prepare a guide solely with several possible disruptive scenarios followed by mitigation plans and best practices. Incorporation and collaboration with third parties and public organizations are vital for the successful guide implementation. Plan for table-top simulated exercises to determine best response plan.

Principle PR-3: Identify critical assets within the maritime environment.

Most Closely Related to Risk Management

Product: Critical Asset Inventory

I. **Best Practice PR3-1**. Develop a benefit cost analysis tool to assist in selecting the best option for supply chain management.

II. **Best Practice PR3-2**: Identify how the new critical assets can impact the USCG operations.

III. **Best Practice PR3-3**: Conduct review of the previous and new critical assets and identify the types of potential threats can occur on each of them.

IV. **Best Practice PR3-4**: Prepare an internal and external analysis with assets inventory and review and examine how critical assets impact the USCG mission and goals.

Possible Best Practice Enhancements/Future Research: Vessel management is typically done on a first come/first served basis in the ports. What could be done is to better prioritize the ships based on the cargo and goods carried. One possibility is to take a more active vice in queueing vessels for unloading although this may come from port operations. The USCG could use their power to direct this type of prioritizations.

Principle PR-4: Document business practices. (Medium Priority)

Product: Business Practice Report

I. Best Practice PR-4-1. Develop a benefit cost analysis tool to assist in selecting the best option for supply chain management.

Possible Best Practice Enhancements/Future Research:

Prepare a benefit cost analysis plan with financial governmental officials, USCG stakeholders and supply chain professionals for assisting in the development.

Project Background

Resiliency in Supply Chains

Risk: Supply chain management is based on risk – e.g., risks of a disrupting event occurring, of the event being mitigated in a timely and cost-effective manner, of having resources available for mitigation, of environmental factors affecting the mitigation plan, etc. Risk is in and of itself a complicated science because it is predicated on predicting the future by looking at past data. For example, most enterprise risk models did not foresee the COVID-19 pandemic, or if the risk models did account for a pandemic event, did not foresee either the extended pandemic timeline or the consequences cascading through the supply chain. As such, enterprises lacked long-term mitigation strategies.

To prepare for disrupting events, federal entities are required to perform myriad risk assessments and establish plans for the "*what-if*" scenarios. Events in those risk models are first characterized by the risk, its likelihood of occurring, and the resulting impact. At one time, mitigation strategies for events with low probabilities were not considered because of the low probability. With the advent of understanding Black Swan events, this concept has changed. Black Swan events are characterized by three factors: (1) An event with an extremely low probability that (2) if it occurs, has disastrous consequences, where (3) in retrospect, the event and consequences were foreseeable (CFI,2022). The COVID-19 pandemic could be considered a Black Swan event, but the consequences would be the same. What is important is to consider the three aspects: probability, consequences, and foreseeability.

What is most crucial is understanding the time elements of any disrupting events: (1) the time an event is being predicted to determine the time to prepare, (2) the time of the actual disrupting event, and (3) the time of the recovery once the event has ceased. If a disrupting event occurs over a longer period than predicted, it effectively exhausts the resources for mitigation.

Supply Chain Timelines: Supply chains operate effectively if there are more predictable events with adequate time to plan. Certain disrupting events can be prepared more effectively for even if it disrupts the physical flow of the supply chain to effectively mitigate the disrupting event (e.g., a hurricane with adequate warning) versus a cyber-attack with no warning or time to prepare. What provides the most disruption in the supply chain are those events without an adequate warning such as some Black Swan events and cyber-attacks which usually are discovered only by the symptoms of the compromised system.

Supply chains are a complex network where goods are distributed and transported. There are three viewpoints for supply chain networks

1. The *physical goods and cargo flow* whose data is stored, accessed, and analyzed by the *digital information flow*.
2. The *digital information flow* that tracks and monitors the scheduling and transporting of the goods and cargo with the *financial flow.*
3. The *financial flow* that tracks the financial transactions used throughout the supply chain (i.e., procuring, transporting, storing, shipping, executing changes) often by using cost benefit analysis by the respective parties in the supply chain that may not optimize the supply chain.

This research considered only the first two aspects focusing on the digital information flow of the physical goods and cargos.

Supply chains are typically managed by deriving models that predict the flow of physical goods and services managed by the digital information flow contained in information technology (IT) systems that provides near-real time data on the supply chain. These models identify bottlenecks or other symptoms of disruptions and provide visibility into how the supply chain could be manipulated to avoid or mitigate these problems.

Resiliency: To better understand resiliency requires a review of the concept of resilience in the supply chain as the concept is not new but is now being revisited. What is new is the increased focus on resiliency as a mechanism to better manage the supply chain given the challenges of the past few years. Resiliency allows supply chain stakeholders to better manage unforeseen and unpredictable events that influence its productivity, performance, and both the routine and non-routine business operations (Pettit et al., 2019). If the model and resiliency are properly executed, we would expect actions to be less reactive and more proactive as well as more predictive. Hence, concepts of building resiliency into entities are necessary to promote supply chain success, economic prosperity, and national security.

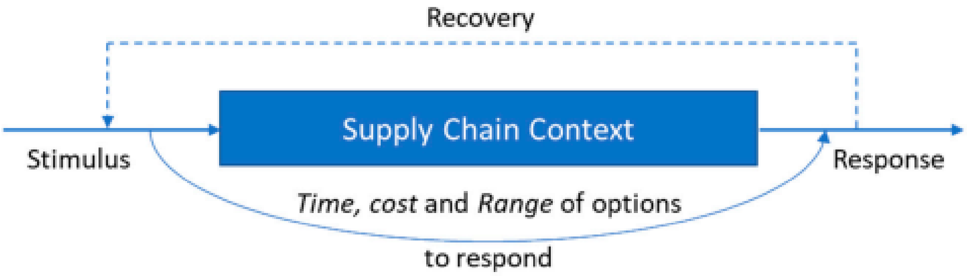
Furthermore, supply chains may be disrupted beyond predictive models during high demand and shifts in market trends causing unforeseen situations for an entity. A sudden supply chain disruption causes a breakdown in the global supply chain cycle. A report by Horne and Shillingford (2021) provided that 84% of the global supply chain was disrupted by delays in cross border land transportation during the COVID-19 pandemic. This high percentage in global supply chain disruption has put a lot of concerns for practitioners who lost 66% of key skills and talent in their workforce (Horne & Shillingford, 2021).

Another salient example occurred with a shortage of computer chips in 2021 – 2022 (CDW, 2022) that resulted in consequences throughout the supply chain including lack of delivery of assets ranging from computers to automobiles. Therefore, planning to become resilient and examining existing processes to either avoid unnecessary disruptions or being able to circumvent consequences of the disruptions are required for the smooth functioning of the supply chain. It cannot be overly emphasized that the success of resiliency will be a thorough understanding of the supply chain network and the availability of timely data to measure traffic flow.

Resilience plays a significant role in systems engineering thinking, psychology, ecology, disaster management, and recently in the global supply chain management as well (Beigi, 2019). Resiliency was originally introduced in 1973 by an ecologist, Holling, who observed resilience's role in some ecological systems (Talubo et al., 2022). He inferred resilience is the ability of entities to absorb and react to environmental disruptions without decreasing performance. From this notion, management and organizational studies found this concept to be able to efficiently and effectively handle supply chains by becoming adaptive, experimental, as well as flexible. The field of engineering has provided a more scientific definition of resilience as it entails the ability of a material to return to its original shape (without deforming) after removing the stress that has brought elastic strain to it (Bostick et al., 2018). This definition provides that resilience is, in fact, a synonym of flexibility and elasticity that involves planned and unplanned options in responding to disruptions. As resiliency moved from physical assets to digital assets, a big focus of resiliency has been in cybersecurity resiliency in both the supply chains and other systems where expected outcomes needed to be maintained during a cyber-attack. As such, many of the concepts used in this research are from the cybersecurity domain because the consequences of supply chain disruption, regardless of the source, are similar.

Resilience entails withstanding disruptive events and managing the supply chain in ways that are exceptional and effective during uncertainty or risky situations. While there may still be consequences to the disruptions, their effect will be as minimized as possible. The effectiveness of resilience lies in its ability to bounce back the supply chain in post disruption period (Wieland & Durach, 2021). The two broad categories of resilience entail resistance and recovery capacity. The resistance capacity refers to the management of an entity in a way that avoids damages and lowers the time between the disruption period and recovery phase. Likewise, the recovery capacity encompasses stabilization processes, measures, and practices opted by an organization in post disruption. This category focuses on quick response during disruption events and minimizing the negative impact between its effects and recovery as well (Chen et al., 2020).

In more classic terms, an entity which is effective and successful in either avoiding or properly mitigating risks and bouncing back speedily is known as “hardy” (Duchek, 2020 as a synonym for resiliency. The term ‘hardy’ is given in the sense that it is harder to break during a supply chain disruption as it is well equipped with unlimited resources and supplier capacity. One long-term research goal not addressed in this work, but which could be useful, would be what constitutes a metric of being “hardy” in a supply chain. In the following diagram, Stimulus is a Disrupting Event with the consequences within the Supply Chain Context. The Response will be what is required to maintain the operational effectiveness and expected outcomes of the supply chain.



Source: (Kopanaki, 2022).

Resilience in supply chain management is usually interpreted in different ways and terms, but for the research our concept of resilience is that during a disrupting event, the supply chain still produces expected outcomes. To measure the effectiveness of the supply chain resiliency, this research is centered on developing a 3-level supply chain resiliency maturity model with metrics to measure the effectiveness at each level. This architecture is discussed further.

Challenges: The challenge to building resiliency in supply chains are based on myriad supply chain factors.

1. **Maritime Transportation Environment:** The entire U.S. maritime supply chain depends on a transportation system that is made up of both private and public assets. These assets include physical assets (e.g., port facilities, vessels) as well as virtual assets (e.g., information technology and operational technology electronic systems).

2. **Conflicting Goals between the Public and Private Sectors:** US policy is predicated on the USCG's mission to ensure safety and security and specifically to "to safeguard the efficient and economical movement of $5.4 trillion in overall economic activity flowing through the Nation's ports and waterways."[10] This requires optimizing over the holistic supply chain. Companies utilizing the ports and waterways are profit-motivated and must be responsive to their stakeholders resulting in decisions optimized locally for their respective entities, but not for the supply chain. This not corporate greed, but focusing on issues such as contracted delivery dates, etc.

3. **Conflicting Missions within the Government:** Myriad government agencies have missions to protect, detect, respond, recover, and investigate disruptions. The specific agencies differ based on the specific disrupting event. These government agencies often have different missions and because of this difference, have different goals and objectives as well as response training and reporting. When a disrupting event occurs, myriad government agencies may be called in to remediate or investigate the incident. For example, an oil spill may require the UCSG, Environmental Protection Agency, the Department of the Interior, the U.S. Department of Agriculture, the National Oceanic and Atmospheric Administration, as well as Secretary of Defense who authorizes the use of state National Guard units. Their roles may range from clean-up to investigations and often involve research teams from other federal entities (e.g., the National Science Foundation).

   A salient example of conflicting missions may arise in the next few years as new legislation is imposed on owners of critical infrastructure assets is that the maritime transportation system (MTS) is part of the Transportation Systems Sector as categorized by DHS. Within the next two years, DHS will require any "significant cyber incident" to a critical infrastructure asset to be reported under recently enacted legislation. Because of the short time reporting requirement, entities may report something as a "significant cyber incident" which, in fact, may not fall under the requirements. It may complicate a response since the required reporting may hinder response and recovery operations.

[10] https://www.uscg.mil/About/Missions/

4. **Supply Chain Complexity:**

   What complicates supply chain resiliency is the conflicting missions and goals of the stakeholders. That is, the competitiveness of the business world is encountering greater threats to the global supply chain, including financial and company viability, cyber security (e.g., data theft, disrupted operations, ransomware), natural disasters (e.g., earthquake, COVID-19, hurricanes), man-made events (e.g., mistakes, explosions, technology malfunctions) and geopolitical events (e.g., tariffs, embargo) that requires effective preparation and planning (response to the situations) in making supply chain resilient (Um & Han, 2020).

5. **Supply Chain Sustainability:**

   With the continuously global and domestic supply chain bottlenecks that cause significant port congestions, the vital role of USCG to provide alternative solutions such as advising for alternative shipping routes and directing vessels to less congested ports for achieving efficacy and less port inventories levels, is of major importance for the sustainability and proper functioning of the ports.

6. **Supply Chain and Digital Transformation:**

Rapid important technology changes have the potential to bring improved efficacy to the supply chain. However, given the myriad stakeholders, this may be less than optimal given that each is implementing their own technologies that may not integrate or interface with other newly implemented technologies. As such, technological digital transformation is a challenge by itself. The USCG with advanced analytics and with the leverage of technology transformation can act on its behalf and mitigate some of the predicted supply chain disruptions.

Our project uses considerable work done in cybersecurity resiliency because of the government focus on circumventing disrupting cyber-attacks due to the elevated risk of attacks and the consequences cyber-attacks cause in the supply chain. Resilience is a concept most often associated with recovering from disasters to provide expected outcomes. In supply chains, resilience ensures the cyber supply chain will provide required products and services and these products and services will be able to sufficiently perform or recover, under stress or failure. (ENISA, 2022). As such, for this project we are defining supply chain resilience as the ability to continue to function with expected outcomes while under a disrupting event (e.g., weather, cyber-attack, pandemic, mistake, accident).

The motivation behind conducting this study is that this report will produce principles and best practices for resiliency in the maritime supply chain applicable to the operational (OT) and information (IT) technologies environment. Towards this purpose, this report will examine United States Coastal Guard (USCG's) resilient supply chain operations for cyber security by using the resiliency model developed under this research (i.e., the maturity model and metrics) described further.

Resilient Supply Chain Architecture: Maturity Model and Metrics

The Supply Chain Capability Maturity Model for the United States Coast Guard

The architecture of the supply chain resiliency model is comprised of maturity model and metrics. The major construct is the maturity model entails three levels--Basic, Intermediate, and Optimized.

For each level, the maturity model defines:

(1) Characteristics of that level,

(2) Processes at that level and to what extent,

(3) Level of documentation required and by what standards.

(4) Associated risks; and

(5) Metrics to monitor performance/capture method.

Level 1 (Basic)

Characteristics: Basic knowledge of the potential disruptive events but lacking a coordinated, repeatable process for dealing with the disruptive events.

The lowest level of the maturity model is categorized as that with minimal resiliency, and thus risks a severe impact by a disrupting event both in terms of operational disruption and length of the consequences of the disrupting event. The processes are reactive and ad hoc; that is, practices that are not well designed optimally and are not repeated. As such, a response is reactive to the salient and often observable symptoms of a supply chain disruption rather than to the actual causes of the disruption. A salient factor in differentiating the levels is the sophistication of the TTPs (tactics, techniques, procedures). One aspect of this level is the lack of a coordinated team for response. Individuals are reacting to symptoms without well-defined tasks to guide their activities.

Initially, supply chain disruption is linked with an unplanned and unstructured set of activities and exercises. The response of supply chain practitioners is reactive that nurtures high risk (uncertain results with additional cost). Organizational structures are not well integrated and not conducive to effect process execution (Kandaperumal et al., 2021). Metrics in this lowest level are typically also ad hoc – based on the ease of collection rather than the applicability to actual improvement. There are minimal efforts to document the TTPS necessary to define the infrastructure for repeatable, traceable processes. This inefficiency results in considerable costs to the entity in terms of actual expenses and time.

Result: Disrupting event could have severe impact on the USCG'S supply chain

USCG can attain and sustain defined performance improvements while having known the change in impact, likelihood of the event, strategies for mitigation, and estimated residual risk.

Level 2 (Intermediate)

Characteristics: Proactive, managed processes with an acceptable level of risk and built on standards. More sophisticated capabilities aligned with best practices and the acceptable level of risk.

In the second level, the performance and productivity improved with the implementation resilient supply chain practices. It involved moderate risk where the response is less reactive than level 1, Ad Hoc. The supply chain practitioners assign duties to each process unit irrespective of the functional units. The organization structure becomes horizontal (ideal for supply chain operations) (Masuda, 2021). Stakeholders throughout the organization are encouraged to collaborate both within and outside of organizational boundaries (e.g., suppliers, distributors, transporters, and consumers). Furthermore, customers engage in supply chain improvement efforts that yield higher efficiency as well (Venkataramanan et al., 2020). Hence, supply chain practitioners can achieve balanced resilience where a portfolio of capabilities is matched with the patterns of vulnerabilities.

By comparison, the middle level of the maturity model risks more of a moderate impact by a disrupting event. There is some level of resiliency because the processes are more repeatable than the lowest level, but are not optimized. There is some monitoring of identified risks, but the risk assessment is either inadequate or the supply chain management may be hampered by a lack of access to readily available data. A response is coordinated because a plan is documented with the risk, probability, impact assessments and established TTPs. The difference between the middle and optimized levels lays in the ability to do more analysis to be less reactive.

Result: Disrupting event could have a moderate impact on the USCG'S supply chain

USCG can attain and sustain defined performance improvements while having known the change in impact, likelihood of the event, strategies for mitigation, and estimated residual risk.

Level 3 (Optimized)

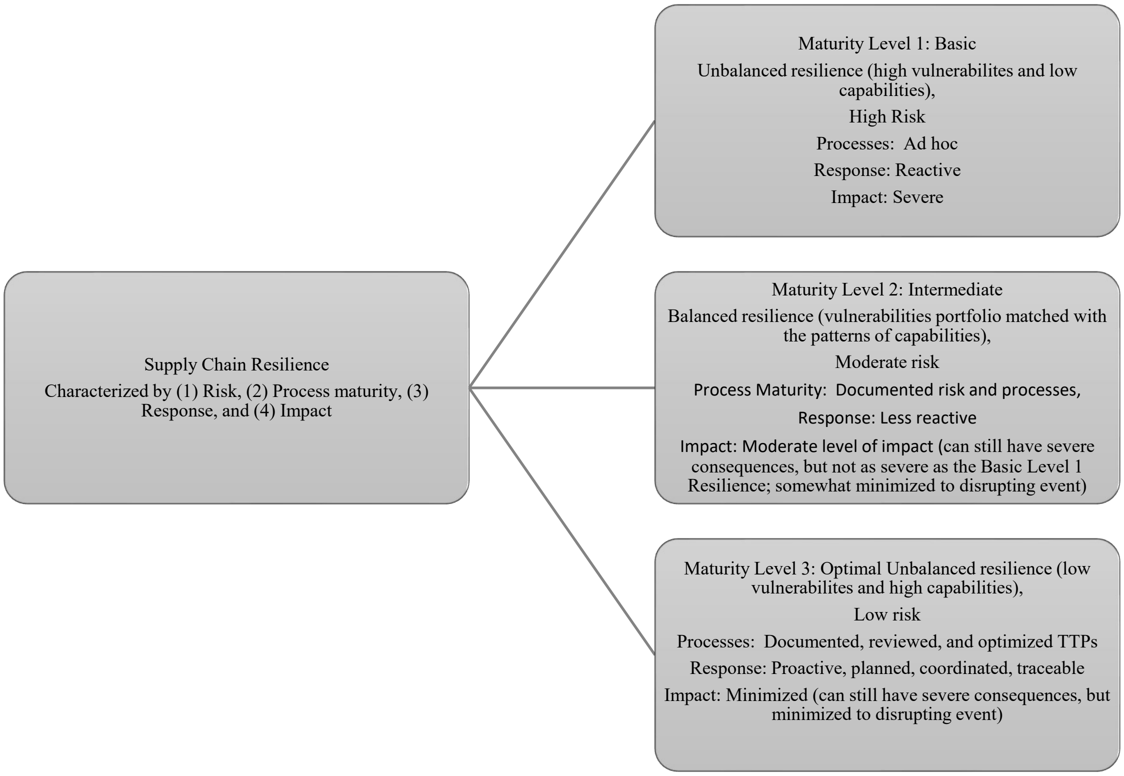
Characteristics: Optimized processes improved by measurement and control for continuous process improvement. An instilled culture of continuous monitoring and upgrading of processes. Activities that are evaluated, repeatable, and have confirmed effectiveness

The third level, Optimized, the risk is quite low with the proactive response of supply chain practitioners. This level is characterized by integration, where supply and customer base form alliances. Teams from multi departments and organizations form alliances with extended planning activities to improve performance and gain the trust of supply chain stakeholders. The organizational structure becomes horizontal (hierarchy and functions operate on supply chain management practices) with applicable process measurements (Kandaperumal et al., 2021). The traditional practices of the supply chain diminish with strategies and resilient substitution. With resilient practices, process improvement takes place with cost reduction as well. Customer satisfaction is headed priority to achieve a competitive edge. The elements that are measured in the third level involve trust and process performance thoroughly. The returns, investment, and cost are shared in this system improvement process. The competitive advantage is achieved through the alliance and integration of multi-organizational supply chain stakeholders (Masuda, 2021). Hence, the firm can achieve low vulnerabilities and high capabilities that is ideal in becoming a resilient supply chain.

The highest level is optimized with minimal impact. It is important to note that there may be significant impacts, but the resiliency minimizes the impacts as much as possible. At this level, optimized TTPs are in place for coordinated response. This includes performing an after-actions "lessons learned" assessment to continuously improve the TTPS for subsequent disrupting events. The response is proactive, not reactive and utilizes a supply chain disruption playbook such as the principles and best practices. Further, there are designated response roles for coordination and a team with assigned tasks and responsibilities.

Result: Disrupting event could have minimal impact

These three levels are summarized in the following figure.



Supply Chain Resilience
Characterized by (1) Risk, (2) Process maturity, (3) Response, and (4) Impact

Maturity Level 1: Basic
Unbalanced resilience (high vulnerabilites and low capabilities),
High Risk
Processes: Ad hoc
Response: Reactive
Impact: Severe

Maturity Level 2: Intermediate
Balanced resilience (vulnerabilities portfolio matched with the patterns of capabilities),
Moderate risk
Process Maturity: Documented risk and processes,
Response: Less reactive
Impact: Moderate level of impact (can still have severe consequences, but not as severe as the Basic Level 1 Resilience; somewhat minimized to disrupting event)

Maturity Level 3: Optimal Unbalanced resilience (low vulnerabilites and high capabilities),
Low risk
Processes: Documented, reviewed, and optimized TTPs
Response: Proactive, planned, coordinated, traceable
Impact: Minimized (can still have severe consequences, but minimized to disrupting event)

Table 1: Maturity Model for Supply Chain Resiliency

Metrics

Metrics, often called Key Performance Indicators (KPIs), are used in tracking, envisioning, and improving supply chain operations efficiently and effectively (NIST SP 800-55, Vol 2; Bharti & Mishra, 2020). They are, in addition to other uses, assist supply chain entities in measuring growth and development of their capability to manage supply chain disruptions. Metrics focuses on continuous supply chain improvement by reducing lead time, deploying resources with minimum waste, automating processes, and speedily recovering from failures. They are used to enhance accountability and improve performance through effective and rational decision making by supply chain practitioners (Behzadi et al., 2020). Metrics are analyzed from multiple perspectives (present and past performance) to gain a fuller understanding of the future performance by tracking all the possible and applicable metrics, needed for business growth and process improvement (Ram et al., 2019). Hence, with robust research (data collection, analysis, and reporting performance-related data), gaps and disruptions in the supply chain are effectively addressed by using metrics.

Metrics must be able to be collected, analyzed, and monitored over time. One limitation of this research was not defining the specific metrics, but this research identified categories of metrics as shown in the Table 1 below.

Category of Metrics	**Data Availability** **How to Collect or Measure**	**Consequences**	**How Used**
Identified and Quantified Risks	Collect data from monitoring of USCG's consistent and continuous risk assessment activities for tracking IT/OT systems of ports (offshore, onshore, and onboard) (Tuomala, 2021). Risks assessments are required under prevailing federal law.	Influences port and vessel operations by events that occur that are not properly identified or mitigated in a risk assessment and consequently may disrupt operations.	Improving AIS port systems and implementing a resilient cyber security management tool in landside operations. The goal is to strengthen connections along with landside and waterside port facilities. Port system activities from Waterside and landside will be connected.
Man-made incidents including errors and mistakes	Collect data from USCG systems that control infrastructures such as cargo security, the backing of assets, and port calls (Bichou, 2015).	Influences routine and non-routine operations of vessels, ports, and traffic operations with uneven supply chain due to loss of data unintentionally.	To minimize human errors by using PMS to assure a smooth and efficient supply chain along with USCG's port facilities and their uninterrupted port coordination by using metrics of "Incident Handling Control" **IR04 Incident response** (NIST SP 800-160, Vol.2)) (Ross et al., 2021).
Natural and physical incidents	USCG establishes best Safety practices plan to cover most contingent natural and non-natural events with guidelines for immediate action (Including new guidelines for pandemics) (Moraci et al., 2020).	Influence handling operations at port, floating of containers, electrical	In planning safety practices for contingent natural and non-natural incidents with guidelines for immediate action. Opting for smart ports (Artificial intelligence) in

		equipment of ports, and flooding accumulation on terminals etc.	detecting unforeseen disruptions (Allen, 2011). Important metrics in this domain are datasets for tracking different unforeseen events, latest/updated sensors, while using and updating already established systems (Radio fax charts and USCG Maritime text forecasts, etc.).
Supply Chain Management	Analyzing and evaluating any breach of agreements, protocol, and standards of third party with USCG. Reviewing annual protocols, limitations, and breach of agreements by third parties. Identifying third party suppliers. Monitoring IT/OT systems for tracking breach, Consistent detection by USCG for Integrity Checks and Provenance Tracking (SR-5, SR-11) (Allen, 2018).	Any third-party port systems control impacts overall port operations at USCG negatively.	USCG, together with the port ecosystem, build approved supplier list with security guidelines, mitigation measures in case of disruptions/ Furthermore, they should implement programs for monitoring supplier's networks as well.
Other supply planning disruptions	From having full control of port ecosystem (Port Supply chain systems) and monitoring the landside operations as well.	Influence optimization of ports such as stock pilled containers and cluttered ports as well.	Using predictive analytics, simulation like VISSIM (preventing disruptions and measuring impact in landside operations), and automation in finding suitable truck drivers (Joh, 2017).

Table 1: Metrics Characterizations

Possible Scenarios for Disrupting Events

Scenario: Cyber-attacks events against port systems

Definition: Cyber-attacks events against port systems (both OT and IT systems)

Process: IT/OT Systems (including servers, software applications, all hardware including highly automated systems) and the overall Marine Transportation system, (MTS).

OT interrupt operational processes.

USCG needs to have a risk assessment of the digital assts (e.g., hardware, software, and how such events may impact ports.

Targeted Assets: IT/OT Systems including servers, software applications, all hardware including highly automated systems and the overall Martine Transportation Systems (MTS). Examples: Intrusions into telecommunications equipment, networked systems linked to cargo control etc. Also, other malicious software that can impact mission site servers that are linked to security functions.

Key Responder: USCG Organization: Cybersecurity Operations Center and Network Operations Center (https://www.dco.uscg.mil/Our-Organization/CGCYBER/)

Red Team ready to regular reviews of USCG Policies, Procedures, obligations of Information technology. USCG Stakeholders and the assigned Port Cyber Security officers. Direct persons/ teams responsible for this operation. Port State control officers (PSOs), Cyber Protection teams (CPTS), Maritime Cyber Readiness Branch (MCRB), Field Cyber Mission Teams, and Port operational commanders.

Detection of Disrupting Event: Constant monitoring of both IT and OT systems for indicators of compromise including USCG systems.

USCG ready to constantly detecting /monitoring network loopholes, on USCG systems such as AIS, E-Noad, C-TPAT, for preventing disruption to the Maritime transportation system (MTS).

Motivation for Response: If not properly responded, the event can result in closure of port facilities and operations. That even could shut down several ports as the malware spreads.

Risk Assessment:

High likelihood of the event causing major consequences if not managed within reasonable time limits.

Low likelihood of the event if constant monitoring is done.

References: Sources including CVC-WI-027(2) (2021) & USCG – Cyber security outlook (2019)

Scenario: Physical / Natural and Man-made Events

Definition: Physical/ natural and manufactured events which have Impact on seaport and intermodal infrastructure

Process: Natural events such as Hurricanes, storms, floods, earthquakes, and manufactured events such as fire in facility port terminal, container explosion in the port warehouse, even accidental collapse of a port facility.

Target assets: Port Terminals, Port Warehouses, Port railways, Port Equipment, Cranes, and transiting cargo/assets.

Key Responder: USCG CG-FAC office of Port & Facility compliance specific departments: Port Resiliency/Recover, Critical Infrastructure (Cyber security, AMSC and PSS), Facility Security MTSA (, and Facility safety).

USCG Port resiliency officers, critical infrastructure officers, port commanders, Captain of the Ports (COPT), Marine Inspectors and Port state Control officers (PSCOs).

Detection of Disrupting Event: USCG should have the latest version or amplify existing sensors/datasets according to the USCG standards. (i.e., seismic, vibration, water line and fire sensors).

Information can also be received from third party organizations informing for natural events. Constant deployment of Natural detection systems.

Motivation for Response: Contingent natural and non-natural events. The events are usually contingent or can happen accidentally, i.e., port facility fire.

Risk Assessment: High probability if not managed on time, or not precautionary measures – full contingency plans have been taken or understood.

Medium likelihood of the event by establishing best safety guards

References: Sources including CVC-WI-027(2) (2021)

Scenario: Systems damages/ destructions

Definition: Systems damages/ destructions on Power Equipment, Cabling of main systems, systemic breakdown of terminal facilities.

Process: System entity – unpredictable malfunction of the system itself or causing effects to the system from other sources.

Target assets: Systems like Sensors, Cranes, supply devices, equipment for terminals, etc.

Key responder: USCG Cyber security officers, Port bridge officers, Port Engineers working in conjunction with USCG.

USCG organization: Critical Infrastructure (Cyber security, AMSC and PSS), Responsible- Port/Terminal operators).

Detection of Disrupting Event:

Infrastructural intervals. Port officers shall monitor the systems and having sub-systems for reducing risks to the main systems. Situational awareness and performance resilience engineering are key factors for proper detection. Systems maintaining and testing main systems such as PCS, CCS, (ENISA).

Motivation for Response: No systematic monitoring of the systems can lead to damages and consequently port disruption and overall supply chain.

Risk Assessment: High likelihood of the event if no advance monitoring/detection is undertaken or if there is not substantial understanding of system monitoring before the damage.

Medium likelihood if managed on time and if there is advanced awareness, steps are taken, and protocol standards exist and are followed.

References: Sources including CVC-WI-027(2) (2021)

Scenario: Unintentional damage/Human error

Definition: Unintentional damage/Human error. Damage of port hardware systems and consequently operational system damages of port facilities. Damage of USCG and Port systems.

Process: PMS (Port Management system), USCG Logistics information management system, and port facilities.

Port Facilities, IT, and administration staff when processing role-based work.

Target assets: PMS (Port Management system), USCG Logistics information management system, and port facilities and systems.

Key responder: USCG IT/ Cybersecurity and Port IT workers should also include all levels of organization for avoiding such events.

USCG organization: USCG CG-FAC office of Port & Facility compliance. Departments: Critical infrastructure (Cyber security, AMSC and PSS). Cargo and Facilities (CG-FAC-2).

Detection of Disrupting Event: Detected from USCG critical infrastructure officers, Port system officers, incident officers, port protection officers and all employees on duty. Employees shall be aware of their actions and what should be avoided from their side.

Motivation for Response: Unintentional system damage from employee Human error. Usually there is not an intention for damage.

Risk Assessment:

High probability if action is not managed on time from duty officers or if there are not back up plans or awareness procedures to be followed on such incidents.

Medium likelihood there is awareness of Incident handling control and immediate reaction of Personnel on duty is undertaken.

References: Sources including CVC-WI-027(2) (2021)

Scenario: Supply Chain Control (Port control systems)

Definition: Supply Chain Control (Port control systems).

Process: Port operational areas and port system controls. Port systems such as port management information systems (PMIS).

Third Parties such as Security systems companies can cause unintentionally or intentionally damage to port systems.

Target assets: Port operational areas and port system controls.

Key responder: IT Officers, all USCG employees and officers with roles such as Incident Protection officer who is always on duty. Facility officers, Marine Inspectors (MI) and Captain of the Ports (COPT).

Detection of Disrupting Event: Detected by monitoring port systems and operational areas within regular time periods or alternatively, due to detecting data (either by signature or anomalies) to determine if they systems are properly functioning or if any malfunctions are detected.

Motivation for Response: A human-caused hardware malfunction affects the network communication between another one port terminal to another and as a result, brings congestion to the containers schedules.

Risk Assessment:

High probability if there is not continuous monitoring/detection by USCG or port officers for integrity Checks- Provenance Tracking (SR-5, SR-11). Also, if agreements have not been set up with clauses for validating the security standards of the third parties and there is unlimited access to the port systems. (ENISA).

Medium likelihood of the event if limited access is given to third parties. USCG shall have full control of the port systems and the access should be limited and granted on-demand with time limits only to third parties such as Security systems and PCS. (ENISA).

References: ENISA & NIST

Roadmap for Future Research

This project was limited in scope and resources. The key outcome from this project is the conceptual framework of a supply chain maturity model where advances between levels are accomplished by metrics. As well, this project has identified key components of a resiliency model.

1. Dependencies in the supply chain
2. Awareness and new emerging technology can improve supply chain resiliency
3. Potential risk supply chain factors can be mitigated by conducting appropriate plans
4. Disrupting events can be detected by USCG by following best practices and principles
5. The supply chain resiliency maturity model with metrics can measure the effectiveness of the supply chain resiliency.
6. Appropriate controls can minimize the consequences of disrupting events and strengthen the resilience of supply chain.
7. A resiliency maturity model can be used by the USCG for avoiding and mitigating high and non-high disrupting events. Future research can include more examples of disrupting events while utilizing a resiliency maturity model.

Appendix 1: The United States Coast Guard (USCG)

The United States Coastal Guard (USCG) is headquartered in Washington, D.C. Its mission is to aid in navigation, defense readiness, operations, port and waterway security, law enforcement, search and rescue, maritime safety, and stewardship as well (Reyes, 2019). The USCG's safeguards the "Marine Transportation System (MTS)" and “US ports” without disrupting the flow of maritime commerce unevenly. The MTS is an interconnected network in USCG that comprises of 361 ports in 25000 miles of inland and coastal waters and rivers (USCG, 2018). It is providing more than 2.3 million sustained jobs and earning annual revenue of $ 4.6 trillion with its economic activities (USCG, 2018). Its maritime transportation cargos are known as efficient, economical as well as environmentally friendly, which connects the US consumers, producers, farmers, and manufacturers with the global supply chain and markets. Moreover, it provides significant security sealift, vital in supporting logistical requirements of the US military and its nation as well.

In case of supply chain disruption in USCG, the control of information should be agile and resilient to make informed decisions based on best practices of resilience and recovery technologies. The USCG must maintain their supply chain agile within a framework that is able to anticipate and respond immediately during disruptions (Alfaqiri et al., 2019). However, the USCG mission is challenging due to both factors that the USCG has control of – and those the USCG does not have control of – in a maritime environment of both public and privately owned assets. The maritime environment operates within a highly complex networked system controlling both IT and OT assets, physical and virtual systems and assets and their operations, and both legacy and emerging technologies. Further, there is a rush to insert technologies (e.g., automation, robotics, and artificial intelligence) by stakeholders that may optimize the localized operations are not optimized for the holistic viewpoint of the USCG. Furthermore, new, and modernized methods and processes of offshore natural resources exploration are adding complexities to a smooth and efficient global supply chain (Sabri, 2019). Any synthetic or natural disruption can cause significant long-term devastating effects on the supply chain (domestic and global), the US national economy, and security as well.

On the other hand, the USCG’s port ecosystem comprises of port operations stakeholders, including transport companies (railway, shipping, or air), port managing bodies (facility operators, port authorities, and terminal), national authorities (cities, police, and custom), and all other related service providers that are vital in the smooth port supply chain operations including energy and oil companies (USCG, 2018). The technology supply chain to these posts involved safety and security, hardware, mobile and fixed infrastructure, software facilities, network and communication facilities, service providers, and cyber-related assets. Any disrupted technology (information and operation) event to one stakeholder will cause catastrophic information flow disruption throughout USCG (LeBlanc, 2021). Hence, USCG should acknowledge that good practices of the resilient supply chain in the maritime port ecosystem should encompass Operational Technology (OT) and Informational Technology (IT) systems as well.

References

United States Government Standards

NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations (2nd draft), October 2021, available at https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft.

NIST SP 800-160, Volume 2, Revision 1, September 2021, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, available at https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final.

NIST SP 1800-11, September 2020, Data Integrity: Recovering from Ransomware and Other Destructive Events, available at https://csrc.nist.gov/publications/detail/sp/1800-11/final.

NIST Manufacturing Extension Program, available at https://www.nist.gov/mep/supply-chain.

Global Standards:

Cyber Risk Management for Ports: Guidelines for Cybersecurity in the Maritime Sector, December 2020, European Union Agency for Cybersecurity (ENISA) available at https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports.

United States Government Sources:

Executive Order on America's Supply Chains, February 24, 2021, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

National Strategy for Global Supply Chain Security, January 2021, archived content available at https://www.dhs.gov/national-strategy-global-supply-chain-security.

Industrial Sources:

Alfaqiri, A., Hossain, N. U. I., Jaradat, R., Abutabenjeh, S., Keating, C. B., Khasawneh, M. T., & Pinto, C. A. (2019). A systemic approach for disruption risk assessment in oil and gas supply chains. *International Journal of Critical Infrastructures*, *15*(3), 230-259.

Allen Sr, C. H. (2018). Developing and implementing a maritime cybersecurity risk assessment model. *USF Mar. LJ*, *31*, 77.

Behzadi, G., O'Sullivan, M. J., & Olsen, T. L. (2020). On metrics for supply chain resilience. *European Journal of Operational Research*, *287*(1), 145-158.

Beigi, S. (2019). A road map for cross operationalisation of resilience. In *The Science of Hormesis in Health and Longevity* (pp. 235-242). Academic Press.

Black Swan Event. An event or occurrence that is extremely difficult to predict, January 2022, available at https://corporatefinanceinstitute.com/resources/knowledge/finance/black-swan-event/.

Bichou, K. (2015). The ISPS code and the cost of port compliance: an initial logistics and supply chain framework for port security assessment and management. In *Port Management* (pp. 109-137). Palgrave Macmillan, London.

Bostick, T. P., Connelly, E. B., Lambert, J. H., & Linkov, I. (2018). Resilience science, policy, and investment for civil infrastructure. *Reliability Engineering & System Safety*, *175*, 19-23.

CDW, Global Chip Shortage 2022: What Should Your Business Do?, January 2022, available at:

https://www.cdw.com/content/cdw/en/articles/datacenter/global-chip-shortage-2022.html .

Chen, C., Xu, L., Zhao, D., Xu, T., & Lei, P. (2020). A new model for describing the urban resilience considering adaptability, resistance, and recovery. *Safety Science*, *128*, 104756.

CVC-WI-027(2). (2021). Vessel Cyber Risk Management Work Instruction. Available at https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf

Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. *Business Research*, *13*(1), 215-246.

ENISA. (2022). European agency for cyber security. Available at: https://www.enisa.europa.eu/.

Horne FBCI, C., & Shillingford, D. (2021). Supply Chain Resilience Report 2021. Available at: https://www.thebci.org/static/e02a3e5f-82e5-4ff1-b8bc61de9657e9c8/BCI-0007h-Supply-Chain-Resilience-ReportLow-Singles.pdf

Joh, E.E. (2017). Automated policing. *Ohio St. J. Crim. L.*, *15*, p.559.

Kandaperumal, G., Linli, J., Pannala, S., & Srivastava, A. (2021, April). Rt-rms: A real-time resiliency management system for operational decision support. In *2020 52nd North American Power Symposium (NAPS)* (pp. 1-6). IEEE.

Kopanaki, E. (2022). Conceptualising Supply Chain Resilience: The Role of Complex IT Infrastructures. *Systems*, *10*(2), 35.

LeBlanc, E. G. (2021). The Case for Offshore Wind: Offshore Wind and the US Coast Guard Maritime Commerce Strategic Outlook. *Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council*, *78*(2).

Masuda, Y. (2021). Adaptive Integrated Digital Architecture Framework: Risk Management Case. In *Architecting the Digital Transformation* (pp. 223-245). Springer, Cham.

Moraci, F., Errigo, M.F., Fazia, C., Campisi, T. and Castelli, F. (2020). Cities under pressure: Strategies and tools to face climate change and pandemic. *Sustainability*, *12*(18), p.7743.

Ram, P., Rodriguez, P., Oivo, M., & Martínez-Fernández, S. (2019, May). Success factors for effective process metrics operationalisation in agile software development: A multiple case study. In *2019 IEEE/ACM International Conference on Software and System Processes (ICSSP)* (pp. 14-23). IEEE.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. J., & McQuaid, R. M. (2021, December). NIST Special Publication 800-160, Volume 2 Revision 1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. In *National Institute of Standards and Technology (US)* (No. NIST SP 800-160, Vol. 2, Rev. 1; National Institute of Standards and Technology Special Publication 800-160, Vol. 2, Rev. 1). National Institute of Standards and Technology (US).

Sabri, E. (2019). Transformation Framework for Supply Chain Segmentation in Digital Business. In *Technology Optimization and Change Management for Successful Digital Supply Chains* (pp. 54-84). IGI Global.

Talubo, J. P., Morse, S., & Saroj, D. (2022). Whose resilience matters? A socio-ecological systems approach to defining and assessing disaster resilience for small islands. *Environmental Challenges*, 100511.

Tuomala, V. (2021). Maritime cybersecurity. Before the risks turn into attacks.

Um, J., & Han, N. (2020). Understanding the relationships between global supply chain risk and supply chain resilience: the role of mitigating strategies. *Supply Chain Management: An International Journal*.

USCG. (2018). MARITIME COMMERCE STRATEGIC OUTLOOK. Available at: https://media.defense.gov/2018/Oct/05/2002049100/-1/-1/1/USCG%20MARITIME%20COMMERCE%20STRATEGIC%20OUTLOOK-RELEASABLE.PDF.

Venkataramanan, V., Sarker, P. S., Sajan, K. S., Srivastava, A., & Hahn, A. (2020). Real-time federated cyber-transmission-distribution testbed architecture for the resiliency analysis. *IEEE Transactions on Industry Applications*, *56*(6), 7121-7131.

Wieland, A., & Durach, C. F. (2021). Two perspectives on supply chain resilience. *Journal of Business Logistics*, *42*(3), 315-322.

Cyber-Maritime Resources:

Bookings. How to build more secure, resilient, next-gen U.S Supply chains, December 2020. Available at: https://www.brookings.edu/techstream/how-to-build-more-secure-resilient-next-gen-u-s-supply-chains/.

Cyber Security Risks in Globalized Supply Chains: Conceptual Framework, October 2019, available at https://www.researchgate.net/publication/338668641_Cyber_security_risks_in_globalized_supply_chains_conceptual_framework.

National science foundation. Understanding the mechanics of global supply chains., November, 2018, available at: https://beta.nsf.gov/science-matters/understanding-mechanics-global-supply-chains

New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain, October 2021, available at https://www.tandfonline.com/doi/full/10.1080/00207543.2021.1984606.