Abstract – This document presents a comprehensive analysis of the multifaceted impacts of cyber-physical attacks on seaport operations, with a focus on quantifying econometric losses. The analysis will delve into various aspects, including the direct economic losses incurred, the ripple effects on different industry sectors, the specific vulnerabilities and consequences of cyber-physical attacks, and the security measures within maritime ports. This analysis is particularly beneficial for security professionals, IT experts, policymakers, and stakeholders across various industries, offering insights into the magnitude of potential disruptions and guiding the development of robust cyber resilience strategies. The insights gained from this analysis are crucial for enhancing the preparedness and response to cyber threats in critical national infrastructure, thereby safeguarding economic stability and national security.

I. Introduction

The paper titled "Quantifying the econometric loss of a cyber-physical attack on a seaport" presents a comprehensive study on the economic impacts of cyber-physical attacks on maritime infrastructure which are critical components of global trade and supply chains and a significant contribution to understanding the vulnerabilities and potential economic repercussions of cyber-physical threats in the maritime sector.

The core of the research revolves around the development and application of an econometric (EC) model designed to quantify the economic losses resulting from cyber-physical attacks on seaports. This model, referred to as the Cyber Physical Econometric Model (CyPEM), is a five-part framework that integrates various aspects of cyber-physical systems, economic impact analysis, and risk management strategies. The methodology involves a systematic approach to model the initial economic impacts of a cyber-physical attack, which, although starting locally, can have far-reaching global effects due to the interconnected nature of global trade and supply chains.

The results highlight the significant economic vulnerabilities of seaports to cyber-physical attacks. Through the application of the CyPEM, the researchers were able to quantify the potential econometric losses, demonstrating that the economic impact of such attacks can be profound, affecting not only the targeted seaport but also the broader global maritime ecosystem and supply chains. The model's findings underscore the cascading effects of disruptions in seaport operations, which can lead to substantial economic losses both locally and globally. It serves as a concrete example of how the model can be used to estimate the economic fallout of cyber-physical attacks on seaports.

It also highlights the convergence of IT and Operational Technology as a transformative force in the maritime sector, creating digital supply routes and modernizing maritime operations. However, this convergence also enlarges the cyber-threat surface, making critical maritime infrastructure more susceptible to cyber-attacks. The threat is not only from common cybercriminals but also from nation-state actors and organized crime groups that possess the resources and motivation to target Critical National Infrastructure (CNI), such as large-scale Cyber-Physical Systems, which include vital maritime operations.

A. Benefits of the proposed solution:

- Quantifies the potential economic impact of a cyber-physical attack on a seaport, both locally and globally
- Helps to identify potential vulnerabilities and weaknesses in the supply chain, allowing for better preparation and response to cyber-attacks
- Can be adapted to analyze different cyber-physical systems

B. Drawbacks of the proposed solution:

- Small sample size of the survey used to gauge public perception of cyber-physical risk in maritime transport
- May require specialized knowledge to use effectively
- Complexity of the model may make it difficult for some stakeholders to understand and utilize the results
- Does not consider other potential consequences of cyber-physical attacks, such as environmental or safety impacts.

C. Application

The proposed framework is useful for quantifying econometric losses resulting from a cyber-physical event. The econometric outputs of a cyber-physical attack on the port allowed for a comparison of the actual risk for cyber-security to the public's perceived risk concerning maritime cyber-threats and how it affects them.

Moving forward, the tool can be used by stakeholders to better quantify and understand their specific cyber-physical risks, including insurance-related corporations with regional and/or global exposure to contingent business interruption losses and organizations whose industrial activity is exposed to global supply chains. The ability to exchange individual framework steps also allows for the modeling of other sectors besides marine and maritime scenarios and the consideration of cyber-physical interruptions at different nodes.

Governmental organizations, port authorities, freight transport and logistic actors, and trade associations may also be interested in the proposed framework, as it can help policymakers gain a greater understanding of their risk landscape and identify particular weaknesses or dependencies

that, if exploited, could have a significant impact on the national economy. Compliance with international governance frameworks, such as the European Union's National Intelligence Service (NIS) Directive, also requires the identification of essential services providers.

The main limitation of the survey was the number of participants, and future work could push the survey to a wider audience and employ cyclic networks when modeling supply chains. Different cyber-physical risk assessments or throughput simulations could also be used to calculate the EM of other sectors or locations. As a cyber-attack can attack the same system in divergent geographic "nodes," modeling and assessing the EM loss could provide novel results.

II. Maritime Cyber-Security

Maritime cyber-security is an increasingly important area of concern for the maritime industry, as emerging technologies such as the Internet of Things (IoT), digital twins, 5G, and Artificial Intelligence (AI) are becoming more prevalent in the sector. The convergence and digitization of Information Technology (IT) and Operational Technology (OT) have driven the transformation of digital supply routes and maritime operations, expanding cyber-threat surfaces.

The integration of digital technologies into critical operations in the maritime sector introduces significant cyber-physical vulnerabilities that could lead to larger global disruptions. As the maritime sector accelerates into digitization, it is critical to understand and quantify the potential impacts of cyber-physical disruptions.

A. Key Points

- Increased marine traffic and larger ships with more capacity have led to challenges in maneuvering in existing channels and seaports, lowering safety margins during cyber-incidents. Today's ships are also more heavily instrumented, increasing the threat surface for cyber-attacks.
- The US Coast Guard reported a 68% increase in marine cyber-incidents, and recent studies show that cyber risks within marine and maritime technology are present and growing as new solutions are adopted.
- While digitization in shipping offers productivity gains, physical safety, lower carbon footprints, higher efficiency, lower costs, and flexibility, there are vulnerabilities in large CPS sensor networks and communication systems.
- A survey of mariners found that 64% of respondents believed that a port had already experienced significant physical damage caused by a cyber security incident, and 56% thought a merchant vessel had already experienced significant physical damage caused by a cyber security incident.

B. Secondary Points

- **Emerging Technologies**: The maritime sector is adopting new technologies across offices, ships, seaports, offshore structures, and more. These technologies include the Internet of Things (IoT), digital twins, 5G, and Artificial Intelligence (AI).
- **Supply Chain Digitization**: Supply chains are also using more Information Technology (IT), introducing digital vulnerabilities. The convergence of IT and Operational Technology (OT) is transforming digital supply routes and maritime operations, expanding cyber-threat surfaces.
- **Cyber Threats**: Nation-state actors and organized crime have the resources and motivation to trigger a cyber-attack on Critical National Infrastructure (CNI), such as large-scale Cyber-Physical Systems, which include maritime operations.
- **Cyber-Physical Systems**: The integration of physical processes with software and communication networks, known as Cyber-Physical Systems, is a significant part of the maritime sector's digital transformation. However, it also introduces new cybersecurity challenges.
- **Impact of Cyber-Attacks**: Cyber-attacks on maritime infrastructure can have significant economic impacts, affecting not only the targeted seaport but also the broader global maritime ecosystem and supply chains.

III. Cyber-Physical Threat

The maritime sector is increasingly vulnerable to cyber-security threats, which can have far-reaching consequences for other areas due to the interconnected nature of modern transportation. As technology continues to advance, the likelihood of disruptive events caused by malicious cyber-attacks is growing, as evidenced by recent reports and academic research. To understand the potential scale of these disruptions, it is important to examine the impact of major supply chain disruptions on the target of the attack and the rest of the associated supply chain. These events resulted in many business interruption insurance claims, with the majority of claims coming from areas outside of the directly affected regions.

Current cyber defense capabilities are unlikely to prevent all cyber-physical catastrophes, making it crucial to quantify and understand the effects of such events. It focuses on the interdependencies in today's global supply chains and presents an econometric model (EM) that allows organizations to transition from a qualitative assessment to a more robust quantitative treatment of supply chain risk.

The world's manufacturing supply networks are susceptible to disruption by cyber-attacks, which can propagate through the network and physically and economically affect adjacent, preceding, and succeeding nodes with negative impacts. Cyber-attacks using IT/OT networks and computing systems can cause short-term losses, Denial of Service (DoS), long-term equipment damage, loss of customer trust, delays in shipment, and loss of strategic advantages due to leaks and compromised sensitive information. Digital cyber-attacks can also have real physical consequences, such as unfulfilled demands in supply transportation and manufacturing.

A. Key points

- With the increasing rate of technological growth, there is a growing likelihood of disruptive events triggered by malicious cyber-attacks in the maritime sector.

- Economic and insured losses stemming from supply chain disruptions are among the top emerging risks for global corporations and insurers.
- As current cyber defense capabilities are unlikely to prevent all cyber-physical catastrophes, it is crucial to quantify and understand the effect of such events.
- The research focuses on how major supply chain disruptions affect the target of the attack and the rest of the associated supply chain, presented in a classical graph format of "nodes" representing assets and "edges" connecting nodes.
- The econometric model (EM) allows organizations to transition from a qualitative assessment to a more robust quantitative treatment of supply chain risk.
- Integrating the EM with MaCRA's dynamic cyber-physical risk model, the combined model allows a user to derive quantitative modeled losses to improve understanding of the global supply chain's cyber-physical risks, leading to increased cyber-resilience and system trustworthiness.

B. Realistic modelling

- The case study is based on a European seaport in Spain and a class of container ship that routinely docks at the same port. Both port and ship are modeled from real-world data, from their physical attributes to their digital attributes.
- The Port of Valencia generates nearly 51% of Spain's Gross Domestic Product (GDP) and is a significant player in European and global supply chains that connect Asia and the Americas. Any disruption to this port would result in a direct economic loss to Spain and ripple through different physical nodes and value chains.
- Existing literature on Supply Chain Risk Management (SCRM) provides numerous frameworks and models for types and sources of risks as well as mitigation strategies. However, little is known about supply chain cyber-risks in an Industry 4.0 technology landscape.
- The Econometric Model (EM) by using a fully quantitative model with comprehensive nodal network mapping to accurately represent the end-to-end life cycle of a product and calculate the econometric impact of an existing supply chain network.
- Disruptions within a Cyber-Physical System (CPS), like maritime transportation, can propagate between the physical layers and the cyber layer due to high interconnections and interdependency. Risk factors range from physical to cyber and also static to dynamic.
- The approach uses a more dynamic cyber-physical approach to risk to present quantified results to the public and measure the change in their understanding of cyber-risk regarding global supply chains.

IV. Framework

The framework uses a "hybrid" modeling method that takes partially mapped supply chains and uses predictive analytics to infill the missing parts. This approach avoids the underestimation of risk by capturing hidden vulnerabilities and correlations stemming from the unseen or unknown parts of a given supply chain. The supply chain risk model is the first of its kind, as it is a quantitative model that incorporates global trade patterns and supply networks, product flow mapping, and correlation across different product groups and industries.

The combined CyPEM stages give public and private organizations the ability to stress test their supply chain resiliency by estimating the cost and time to recover after different cyber-attack scenarios. The framework includes quantitative risk models that emulate major components of global supply chains and their uncertainties to estimate time delays and economic losses resulting from contingent business interruption (CBI). Downtime is measured on the order of days or hours caused by cyber-physical disruptions to a given supply chain node.

The framework has been designed to provide some dynamic automation when calculating cyber-physical econometric losses. Some of the cyber-attack scenario variables can be altered "live" during various stages to explore a range of econometric outcomes. The Port of Valencia cyber-physical attack scenario is used to compute a range of econometric losses, based on the severity of the attack and the duration of the delay (i.e., 3, 5, and 7 days). This tool allows users to proactively manage supply chain risks by anticipating interdependencies and correlations in supply chains and the effects of cyber-triggered disruptive events before they can occur. The quantified results are also critical for measuring gaps in perceived vs. actual risk as understood by experts and laypeople.

The framework is designed to provide analytics for different supply chain arcs or sectors and can be used to communicate quantifiable cyber-physical risk to a wide audience.

- **Define Industry, intermediate parts, and final products**: This stage involves identifying the industry, intermediate parts, and final products that are relevant to the supply chain being analyzed.
- **Define Network where nodes are suppliers and edges are product/part flows**: In this stage, the supply chain network is defined, with nodes representing suppliers and edges representing product or part flows.
- **Calculate Disruption using cyber-physical risk assessment and a port throughput model**: This stage involves calculating the disruption caused by a cyber-physical attack using a risk assessment model and a port throughput model.
- **Propagate Disruption in the wider network**: In this stage, the disruption is propagated through the wider supply chain network to assess the impact on other nodes and edges.
- **Calculate the industry loss and loss distributions**: The final stage involves calculating the industry loss and loss distributions resulting from the disruption.

The first two stages of the framework involve creating acyclic network graphs using United Nations Commodity Trade Statistics and EM product flows to establish product dependencies. Once the product dependencies are established, trade data from the UN Commodity Trade Statistics is incorporated to create a network that includes storage and

transportation nodes, as well as the supply chain flow of components based on inter- and intra-industry dependencies.

The next stage of the framework is network definition, which looks beyond product dependencies to consider a country's manufacturing and transportation to determine product flows and arcs. While the model currently uses an acyclic network to represent the flow of products without creating feedback loops, future modeling at this stage can be exchanged for another type of network depending on the end use of the entire framework. Data used to define and create future networks could include the period of data, the flow (i.e., import/export), commodity codes, trade values, net weights, quantity, and statistics from the reporter (i.e., Port of Valencia).

The proposed network is a hybrid one, which merges the product dependency graph (or tree) from stage one and relevant trade data from stage two. This step ensures that the econometric model can account for movements of trade across country and sector boundaries within product categories. The resulting hybrid network is key to determining the econometric losses from a cyber-physical disruption in the later stages of the CyPEM framework. However, one limitation of this method is that the hybrid network is pre-defined, which could mean fundamental changes to the underlying trade models in the longer-term.

Predictive analytics can improve the product dependency graphs in the earlier stages of the framework, which subsequent stages rely on for accuracy and depth of detail. CyPEM collects data from numerous sources and legacy systems to provide a complete view of the supply chain, and subsequent analyses are conducted to uncover useful information and achieve boosted intelligence. Prescriptive analytics are used to automate complex decisions and proactively and dynamically update recommendations based on changing events to take advantage of these predictions and provide added value to the project classification tools. Using these networks to pre-define many of the market and dependency attributes, and how they affect the rest of the network, while keeping the actual disruption events (and all their individual pieces) more dynamic.

The CyPEM framework involves calculating disruptions using two models: a maritime cyber-risk assessment model and a cyber-physical model of the Port of Valencia's throughput. The maritime cyber-risk assessment model takes a cyber-physical attack chain to show a range of potential risks and outcomes, depending on the success of each segment of an attack chain. The attack chain used in this model has been verified with actual data and testbed experiments, which have been cross-referenced with legitimate system vulnerabilities on ships known to enter the Port of Valencia and with the port authorities from Tam et al. (2022) and Tam et al. (2021).

The second part of calculating disruptions is to take the cyber-physical risks and their outcomes, and to predict the overall disruption effect to the Port of Valencia. To do this, a cyber-physical model of the Port of Valencia's throughput was developed. This process is very similar to stages one and two but built for the internal workings of a single port instead of an entire global network. The proposed method allows the model to be more highly detailed, even modeling the individual ships and terminal cranes (including their type) to accurately determine port downtimes in terms of hours and also in percentages.

In order for the throughput model to simulate port operations for the Port of Valencia, certain parameters that describe traffic and flow within the port must be considered. This includes information characterizing the following: (i) arrival process, (ii) average quantity of containers per port call (in Twenty-foot Equivalent Units, or TEUs), (iii) service time distribution per vessel, (iv) proportion of containers destined to be transshipped, and (v) the mean container dwell time. The analysis can be simulated multiple times to output a range of realistic downtime values that correspond to different attack chains and cyber-physical attack outcomes.

The cyber-attack triggered disruption is observed to decrease the production/transportation capability of nodes and have a ripple effect to successor nodes. Again, in an acyclic network, effects progress downstream in a one-way direction. However, if circular supply chains are integrated into the framework as a future next step, disruption patterns and results could be very different. In this instance of CyPEM, cyber-triggered disruptions are propagated through the network in a similar manner to other types of disruptions (e.g., Levalle and Nof, 2017). A global cyber-attack can differ from other natural disaster disruptions, which can be localized geographically, while cyber-attacks tend to occur where the targeted systems are located. Therefore, a single digital threat, such as WannaCry and NotPetya (Branquinho, 2018), could trigger cyber incidences in multiple geographic regions or reach across several sectors (e.g., health, manufacturing) if similar underlying technology is used.