MODELING A CYBER ATTACKS AFFECT ON PORT MIAMI SHIP TO SHORE CRANE CONTAINER PROCESSING

Anthony Crespo

Sysytems Engineering and Operations Research
George Mason University
4400 University Drive Fairfax, VA 22030

ABSTRACT

Seaports are critical nodes of commerce for goods coming into and leaving the United States. According to the American Association of Port Authorities, seaports contributed $5.4 trillion to the economy in 2018 and the importance is only growing. A key chokepoint in seaborne commerce is how quickly shipping containers can be unloaded from, and loaded on to, trans-oceanic ships using ship to shore (STS) cranes. This paper will examine a microcosm of STS crane operations using Port Miami as a case study. It demonstrates how a cyber-attack, affecting even a subset of STS cranes, at the port can incur a cascading backlog paralyzing the ports ability to process container traffic when compared to normal operations.

INTRODUCTION

Port Miami services approximately 2600 Twenty Foot Equivalent Units (TEU), more commonly referred to as shipping containers, per day. To process all of these containers the ports thirteen STS cranes must complete as many movements per hour as possible during its twelve hour work day. A movement is defined as the completed action of a crane picking up a container from the ship, traversing it back to the quay, and lowering it onto an awaiting chassis or the ground. The inverse of this also constitutes a movement. If the port is unable to process even 10% of this amount due to crane maintenance issues, crane failure, unavailable chassis (outside the scope of this project), etc. the backlog can cascade into a system failure delaying cargo schedules, shipping schedules, spoilage of agricultural goods, and costing the economy tens of millions of dollars per day.

With the recent log jam of ships entering the United States due to easing of Covid restrictions, and a pent up demand for goods, the effect on the U.S. supply chain has been commented on ad nauseum. This led me to ask what would the effect on container processing be if a portion of cranes at a major US port was hit by a cyber-attack causing a subset of the cranes to go down for one day or one week.

While the literature has extensively covered crane TEU processing time, economic impact of crane downtime, optimization of unloading schedules, and much more, I was unable to find anything modeling the effect of a cyber-attack on crane infrastructure. As there is no publicly available data on this, I decided a simulated attack on four of Port Miami’s cranes could elucidate possible implications on what to expect for container backlog compared to normal operations.

In the following sections I will discuss how I modeled normal daily operations so I could compare my simulated cyber-attack, the model I created to do this, how I simulated the cyber-attack, the resulting data, and topics for further inquiry.

PROBLEM AND METHODOLOGY

To simulate a cyber-attack on Port Miami and its effect on container through put, I needed to know how many and what types of cranes the port had, average daily TEU throughput, normal processing time of TEUs by the cranes, and average crane downtime due to maintenance to establish a normal operating baseline. The deterministic variables of this project were the number of cranes at the port and the number of maintenance staff available. The stochastic variables were the crane failure rate, the crane repair time, and the daily containers processed.

According to Port of Miami Crane Management, the port has thirteen cranes separated into four general subsets. Three of the cranes were delivered in the late 1980s and are Kocks H frame. The second subset of four cranes were the first major order for Chinese ZPMC cranes in the Western Hemisphere. The final two subsets, consisting of six total cranes, are Super Post-Panamax (SPP) cranes. The only differentiation between the two sets are the time of the orders. To understand the processing time of these cranes I needed to obtain daily container throughput. The Bureau of Transportation statistics in conjunction with the Army Corps of Engineers provided yearly breakdowns of TEU throughput for Port Miami for the years 2016 through 2020. I also noticed that the port observed at least 10 federal holidays. I divided the yearly TEU by 355 to obtain a daily mean of 2242 and then calculated the standard deviation to obtain a value of 71 TEU. From here I ran a 10,000 iteration Monte Carlo simulation to obtain a final daily mean of 2,304 TEU or 192 TEU per hour for my initial arrival time. Since this was an average daily rate a normal distribution of the data was settled up for container arrival time to the port. A future enhancement to this project could seek ship arrival schedules from the port to take into account individual ship arrival time to the ports and measure the TEUs per ship on an exponential arrival distribution for a more granular look.

The next consideration was how to account for the different cranes processing the containers and the effect of maintenance downtime of the different cranes processing rate. Instead of having the containers go to specific cranes initially, an unknown whose data was not available, I had them go through a queue where there was an equal chance for the daily TEU to be processed by anyone of the 13 cranes. After reviewing the literature, Port Miami crane processing time could be best represented as a triangular distribution. The Port of Miami CEO had actually written specifically on this subject and a distribution of (48, 300, 83), all in seconds, was decided on per container.

The container was then sent to one of two possible outputs. It would either go to the sink 99.45% of the time, or it would be sent to a crane maintenance queue .55% of the time to account for average daily downtime of cranes at Port Miami and the delay effect on container processing. If the container was passed into the maintenance queue it was then routed to one of the four possible subsets based on the percentage of total cranes at the port. Each subset was given a triangular distribution based on data from crane operations manuals, decreased efficiency extrapolation based on age, and Port of Miami data. It should be noted that much of this maintenance data was broader than the author would have liked and further research would request specific data from the Port on a crane by crane basis if they were willing to release that to the public. In addition to where the container was routed in the maintenance queue, it was also imperative to know the number of maintenance technicians who were available to work on the cranes at any given time. Port Miami provided a breakdown of their staff positions and I conducted a LinkedIn search to count the number of maintenance technicians the port had. Further research would request specific numbers from the Port authority to account for workers who may not post their positions.

To simulate a cyber-attack on the Port I was intrigued by recent articles discussing Chinese control of routing technologies and installation of backdoors in many of their exports. I decided to simulate a blanket attack on all four of Port Miami’s ZPMC cranes by disconnecting them from the model for the cyber-attack iterations. This then left the port to handle the same level of TEUs but with only seven cranes. To further enhance the gravity of the problem, the number of technicians to service any other maintenance of the other cranes was cut to a single technician. This was to account for the fact that the most likely decision would be that the majority of technicians would be used in an emergency manner to get the four cranes under attack back into operating condition as soon as possible.

RESULTS

Ten iterations were ran on daily (12 hours) port operations under normal conditions. Ten additional iterations were then ran to simulate a week (60 hours) of cargo processing for a total of 20 iterations of the model ran under normal conditions. The same was then done for the model operating under cyber-attack conditions. The results can be seen in the following tables.

Normal Conditions:

Iteration	Arriving Day	Processed Day	Build Up	Build Up x 5
1	2342	2329	13	65
2	2273	2266	7	35
3	2243	2236	7	35
4	2335	2329	6	30
5	2292	2285	7	35
6	2307	2300	7	35
7	2290	2282	8	40
8	2285	2279	6	30
9	2242	2235	7	35
10	2342	2335	7	35
			7.5	37.5

Iteration	Arriving Week	Processed Week	Build Up
1	11587	11583	4
2	11349	11346	3
3	11452	11441	11
4	11540	11531	9
5	11519	11510	9
6	11502	11497	5
7	11372	11364	8
8	11583	11572	11
9	11383	11378	5
10	11566	11554	12
			7.7

Cyber Attack:

Iteration	Arriving Day	Processed Day	Build Up	Build Up x 5
1	2311	2075	236	1180
2	2309	2074	235	1175
3	2275	2113	162	810
4	2299	2098	201	1005
5	2362	2054	308	1540
6	2258	2108	150	750
7	2280	2081	199	995
8	2299	2072	227	1135
9	2290	2077	213	1065
10	2261	2061	200	1000
			213.1	1065.5

Iteration	Arriving Week	Processed Week	Build Up
1	11342	10507	835
2	11502	10493	1009
3	11487	10499	988
4	11647	10467	1180
5	11441	10567	874
6	11519	10621	898
7	11553	10517	1036
8	11623	10473	1150
9	11568	10518	1050
10	11512	10451	1061
			1008.1

CONCLUSIONS

From the data above it can be seen that an average backlog of 213 containers is created if the four ZPMC cranes were to go down for a single day. If this attack caused the cranes to be down for a week this number would increase to over a thousand TEU backlog. Further research could view how this could cause rerouting of container traffic, spillover effects onto the railway, and trucking network, and possible crane redeployment. In addition, maintenance staff was assumed to work five 12 hour days without breaks. A more refined model could take into account scheduling of staff, emergency consultants being deployed, and personnel dynamics needed to mitigate a cyber-attack.

Some of the literature discussed the possibility of spare cranes to mitigate for longer maintenance periods which a cyber-attack could use as a rough analogy. However, the expense of the cranes does not allow for an economical non-utilization rate. Further thought could be placed into hardening the ZPMC cranes by changing out their software, or replacing them with a different type as their working life comes to a conclusion.

REFERENCES

Phan-Thi, Mai-Ha & Ryu, Kwangyeol & Kim, Kap. (2013). Comparing Cycle Times of Advanced Quay Cranes in Container Terminals. Industrial Engineering and Management Systems. 12. 10.7232/iems.2013.12.4.359.

"Workbook:PortProfiles2022explore.dot.gov/views/PortProfiles2022/ProfileDashboard?%3Aembed=y&%3AisGuestRedirectFromVizportal=y. Accessed 5 Dec. 2022.

Park, Nam Kyu & Suh, Sang-cheol. (2019). Tendency Toward Mega Containerships and the Constraints of Container Terminals. Journal of Marine Science and Engineering. 7. 131. 10.3390/jmse7050131.

Crane Data. Crane Management. (2018, November 26). Retrieved December 5, 2022, from https://www.cranemgt.com/crane-data/

Evaluating efficiency of top global container ports. Evaluating efficiency of top global container ports | JOC.com. (n.d.). Retrieved December 5, 2022, from https://www.joc.com/port-news/evaluating-efficiency-top-global-container-ports_20190226.html

Quay cranes in container terminals - Univerzita Palackého v Olomouci. (n.d.). Retrieved December 6, 2022, from https://tots.upol.cz/pdfs/tot/2013/01/02.pdf

"Port of Miami Crane Management | Miami, FL | Cause IQ." Port of Miami Crane Management | Miami, FL | Cause IQ, www.causeiq.com/organizations/port-of-miami-crane-management,651053081/#personnel. Accessed 5 Dec. 2022.

Parker, Barry. "Florida Ports: A Sunny View of the Container Trades." *gCaptain*, 24 Jan. 2022, gcaptain.com/florida-ports-a-sunny-view-of-the-container-trades.

"Ports." *ASCE's 2021 Infrastructure Report Card* |, 17 Jan. 2017, infrastructurereportcard.org/cat-item/ports-infrastructure.