Assessment and Measurement of Port Disruptions
The Team

• Lavanya Marla (co-PI)
• Randall Sandone (Executive Director)
• Gabriel Weaver (PI)

• Glen Salo (President)
• Brian Barnes (Project Manager)
• Kameron Baumgardner (Chief Technology Officer)
• Josh Vertalka (Chief Data Scientist)
Motivation: DHS/USCG

“Following a disruption of port operations, what are the secondary and tertiary effects of the port disruption on other modes of transport (trucking, rail, pipeline, etc.) and what are the economic impacts of such an incident?”
Motivation: USTRANSCOM

- There is a need to be able to conduct **what if** scenarios when different Critical Infrastructure assets are disrupted.
- USTRANSCOM has a variety of *Commercial Strategic Seaports* vital to its global mission.
- There is a need to understand the impacts of disruptions to these ports from a *mission assurance perspective*.
Motivation: Overview of Shipping Ports

- More than 360 sea and river ports in the United States
- More than 90% of US Goods go through these ports
- Modern shipping ports are a nexus of critical infrastructure systems
  - **Communications/IT Sectors**
    - Navigation (Automatic Identification System (AIS), GPS)
    - Automation & Logistics (Terminal Operating Systems (TOS))
    - Physical Access Control (TWIC)
    - Monitoring (Security Cameras, Customs and Border Patrol Systems)
  - **Transportation Sector**
    - Intermodal (e.g. Road, Rail, Air, Ship)
    - Just-in-time supply chain
  - **Energy Sector**
    - Petroleum, Oil, and Natural Gas
    - Electrical Power
Motivation: We must understand these dependencies in order to identify, evaluate, and mitigate risks to the MTS.

- Port stakeholders must understand the primary, secondary, and tertiary impacts of a disruption to a shipping port and its economic impacts.
- Must understand risk relative to interconnections with other critical infrastructures
  - Communications/IT Sectors
  - GAO-14-459, USCG Cyber Strategy
  - Transportation Sector
  - Symbiotic relationships between ports and other modes of transport
  - Energy Sector
  - Electrical power required to run petroleum pumps and gantry cranes
- In order to understand these dependencies, we must model the port as a system and simulate its operations.

Layers are geo-referenced
Disruptions can affect multiple layers
The Maritime Transportation Security Act requires stakeholders to understand and mitigate these risks.

- **Area Maritime Security Committees (AMSCs)** must conduct risk assessments and develop security plans that mitigate risks
  - Individual Ports (e.g. Port Everglades, FL)
  - Regional Sectors (e.g. Miami Sector)
- **Involves a variety of different stakeholders**
  - Captain of the Port (USCG)
  - Port Security & IT
  - Finances and Business Development
  - Local Law Enforcement and Customs and Border Patrol (CBP)
  - Port Tenants: Cargo, Petroleum, Cruise
- **Existing approaches**
  - Maritime Security Risk Analysis Model (MSRAM, USCG)
  - Threat and Hazard Identification and Risk Assessment (THIRA, DHS)
  - NIPP Risk Management Framework
  - NIST Cybersecurity Framework
  - FEMA National Incident Management System (NIMS)
Our team is building a **general software** framework to model specific ports, identify risks, and evaluate mitigations.

Use the framework to build tools to conduct risk assessments and help develop Area Maritime Security Plans.

- Data used to develop framework from fieldwork.
  - ‘Cyber’ (Communications/IT Sectors)
  - ‘Physical’ (Transportation Sector)
  - Provide input and output from other tools (e.g. SABRE, Verizon information sharing platform)

- Integrate existing approaches with dependencies and risks introduced from other Critical Infrastructures
  - Not SSI
  - Not official data
  - Non-government agencies
  - Artificial but realistic data
  - Can configure to operate on actual data for specific ports

- A basis for information sharing and analysis
  - Among stakeholders within individual Ports (e.g. Port Everglades, FL)
  - Among ports within regional Sectors (e.g. Miami Sector)
  - Across different critical infrastructure sectors

- Align, extend, and complement existing risk assessment approaches
  - MSRAM augmented with ‘Cyber’ from NIST Cybersecurity framework for example.

**Milestone 1:** Baseline Operations

**Milestone 2:** Catalog Disruptions

**Milestone 3:** Simulate cascading effects

**Milestone 4:** Measure economic impacts
The Value

- Different port stakeholders need to conduct *what if* analyses
  - Simulate various disruptions of the MTS
  - Understand increased cost of delivery and delays
  - Model the effect of a theoretically possible attack without implementing that attack.

<table>
<thead>
<tr>
<th>Left of Boom</th>
<th>Boom</th>
<th>Right of Boom</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Training Exercises</td>
<td>• Determine the effects of mitigation strategies</td>
<td>• Evaluate response and recovery strategies</td>
</tr>
<tr>
<td>• Area Maritime Security Plans</td>
<td>• Compute optimal mitigation actions</td>
<td>• Evaluate strategies to improve port operations.</td>
</tr>
<tr>
<td>• FEMA Port Security Grants</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Objectives

• Such analyses need to be conducted continually by individual ports for their specific and changing operational, technological, and threat environments.
  • Intelligent adversaries evolve
  • Environments evolve
• A one-time evaluation is not enough.
• Needs to be a robust set of repeatable analyses by which one can perform “what if” analyses.
• Work with sensitive/non-sensitive data.
Outline

• Intro team
• Motivation
• Objectives
  • Baseline Operations
  • Cyber-Physical Disruptions Catalog
  • Simulate Cascading Disruptions
  • Advanced Visualization
• Conclusions
Baseline Operations
Port Everglades (PEV) - Port Operations

Petroleum Operations

Container Operations
Container Operations

1. Trucks coming to pick up goods line up in lanes depending upon which yard they are going to.

2. At the gate, trucks are checked to be sure that they are in the right place at the right time.

3. Containers full of cargo ranging from bananas to shirts are stored in the container yard for import or export.

4. Gantry cranes load and unload cargo containers from ships docked at the terminal.

5. Ships move in and out of the seaway in order to bring goods into (import) and out of the port (export).
BENEATH THE SURFACE: CONTAINER OPERATIONS

Petroleum Pier

Optical Character Recognition (OCR) or Radio Frequency Identification Tags (RFID) are used to identify cargo.

Gantry Cranes – Cyber

Automated Identification System (AIS) is used to identify ships as they come into the port.

Vessels – Cyber

Gantry Cranes – Cyber

Optical Character Recognition (OCR) or Radio Frequency Identification Tags (RFID) are used to identify cargo.

Gate Operating Systems (GOS) help ensure proper access of trucks to the container yard.

Gate – Cyber

Disrupt

Terminal Operating Systems (TOS) help orchestrate the location and movement of cargo from ship, to yard, to truck.

Container Yard – Cyber

Disrupt

Gate Operating Systems (GOS) help ensure proper access of trucks to the container yard.

Disrupt
Example Network: Container Cargo

Source/Destination
Port: Railway station: Warehouse
Container yard: Retail store: Etc.

Pathway

Resource
Gantry Crane: TWIC: Gate: Etc.

Networks

Disruptions
Delays: Restricted Routes: Outages: Increased cost: Etc.
Detailed Tour of **Florida East Coast Railway** with Paul Deitado (FECR) and Sam Harvill (PEV)
Detailed Tour of Florida East Coast Railway with Paul Deitado (FECR) and Sam Harvill (PEV)

**Baseline Operations**
1. Access Gate (International Gate)
2. Admin Building
3. Rail Yard
4. Gantry Crane
5. Container Yard

**Disruption Scenarios**
1. Access gate failure
2. Remote systems access failure
3. Loss of power
4. Hazards with LNG
5. Heavy rains cause ballast erosion
6. Derailment
Simple Example: Cyber Disruption

\((G_{cyber})\): Cyber network

\((G_{trans})\): Transportation road, rail, and seaway network.

<table>
<thead>
<tr>
<th>Commodity</th>
<th>Location</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unleaded Gasoline</td>
<td>Texas</td>
<td>0.50</td>
</tr>
<tr>
<td></td>
<td>Europe</td>
<td>0.40</td>
</tr>
<tr>
<td>Jet/Kerosene</td>
<td>Texas</td>
<td>0.60</td>
</tr>
<tr>
<td></td>
<td>Europe</td>
<td>0.58</td>
</tr>
</tbody>
</table>

Sources:
- CIRI 154
Cyber-Physical Disruptions
Develop a threat catalog for cyber-physical disruptions to the Maritime Transportation System (MTS)

- Catalog theoretically-possible disruptions to the MTS
- Develop a general model(s) that can simulate the effect of disruptions.
- Prioritize disruptions based on:
  - Stakeholder input
  - Economic impact
- Work with stakeholders
  - USCG, DHS, DOT

<table>
<thead>
<tr>
<th>Description</th>
<th>Fault Category</th>
<th>Location</th>
<th>Duration</th>
<th>Exemplars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Data (TOS)</td>
<td>Accidental, Intended (Ransomware/Data Integrity/Malware)</td>
<td>Container Yard, Terminal Operator Gates</td>
<td>Days</td>
<td>Port of Antwerp, 2013</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Intended (Insider Attack, Phishing)</td>
<td>Port or Terminal Operator</td>
<td>Hours</td>
<td>Revenge sewage attacks (2001)</td>
</tr>
</tbody>
</table>
SCENARIO 1: MAERSK RANSOMWARE

We are sorry but maerskline.com is temporarily unavailable

We confirm that some Maersk IT systems are down. We are assessing the situation. The safety of your business and our people is our top priority. We will update when we have more information.

We apologize for any inconvenience this causes you.

Maersk Line team
SCENARIO 2: HACKING TERMINAL OPERATING SYSTEM
Simulate Cascading Disruptions
Simulation Model

**Discrete Event Simulation**: Simulating the behavior of a complex system as an ordered sequence of well-defined events, e.g.,

*<event>* Ship arrives at port. When the gantry crane *<resource>* is available, a container *<event>* is offloaded.

**Optimal Network Flow**: Mathematical derivation of the optimal route (path) for each commodity through the network.

- Economic impact
- “What if” scenarios
- Disaster planning
- Training and exercise
- Prioritization
- Optimization
- Risk management
Discrete Event Simulation Functionality

- Service time (node and edge)
- Resource constraints (queues)
- Minimum path calculation at each event
  - Commodity dependent
- Accumulated costs
- Time to destination
- Simulations are faster than real-time
Use Case

• 7 Shipments over one week
• Each shipment includes a different number of groceries and retail containers
• Cyber attack disables McIntosh gate TWIC
Model

- Commodities may follow different paths
- Disaster paths available
- Functional behaviors
  - Service time
  - Queue
  - Maximum throughput
  - Accumulated cost/time
  - Minimum path
Disruption Effects on Retail
Simulation Model

Discrete Event Simulation: Simulating the behavior of a complex system as an ordered sequence of well-defined events, e.g., <event> Ship arrives at port. When the gantry crane <resource> is available, a container <event> is offloaded.

Optimal Network Flow: Mathematical derivation of the optimal route (path) for each commodity through the network.

- Economic impact
- “What if” scenarios
- Disaster planning
- Training and exercise
- Prioritization
- Optimization
- Risk management
Optimal Multi-commodity Network Flow (ONF)

• Input:
  • Origins and destinations of vehicles
  • Origins and destinations of commodities/containers
  • Travel times on each link
  • Vehicle capacities, commodity volumes

• Output:
  • Paths and schedules for each vehicle
  • Assignment of commodities/containers to vehicles

• Strengths
  • Multi-commodity flow finds movement of multiple entities on network

• Weaknesses:
  • Difficult to solve; for multiple commodities it is complex!
  • Solution time can be high
Minimize travel costs and delay costs

Each vehicle starts at its origin and ends at its destination

Each commodity container is picked up by a vehicle and delivered at its destination

Time of each movement (container) and vehicle is tracked

Vehicles/containers can move after the release time

Capacities of vehicles must be obeyed
Advanced Visualization
Welcome to Everglades!

Organization:
RealII

Username:
Password:

SIGN IN
### Global Throughput

<table>
<thead>
<tr>
<th>Category</th>
<th>Baseline</th>
<th>Simulated</th>
<th>Projected Revenue Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gasoline</td>
<td>4,200 gal/hr</td>
<td>4,200 gal/hr</td>
<td>$ 26,312</td>
</tr>
<tr>
<td>Crude</td>
<td>1,750 gal/hr</td>
<td>1,750 gal/hr</td>
<td>$ 72,402</td>
</tr>
<tr>
<td>Jet fuel</td>
<td>6,730 gal/hr</td>
<td>6,730 gal/hr</td>
<td>$146,007</td>
</tr>
<tr>
<td>Containers</td>
<td>250 TEU/hr</td>
<td>250 TEU/hr</td>
<td>$ 0</td>
</tr>
</tbody>
</table>
Economic Impact of Cyber Disruptions

- Given a disruption to a shipping port what are the economic impacts of the cascading effect?

- Local Impact
  - **Example:** What is the economic impact of a container yard being down for 4 hours if that yard does $1.5m worth of transactions.
  - **Simple Approach:** Compute the change in commodity flow with and without disruption and multiply by the commodity’s price per unit.

- Regional Impact
  - Multiregional study of the economic impact of dirty-bomb attacks in POLA/POLB [Park 2008]

---

**Cyber Insurance Portfolio Analysis of Risk (CIPAR)**

[https://iti.illinois.edu/news/ciri-researchers-develop-risk-assessment-tool-cyberinsurance-market]
Conclusions

- Shipping ports Seaports are vital to our economy.
- These ports are a nexus of critical infrastructure
  - As seen in fieldwork at Port Everglades
- Stakeholders need a common operating picture and integrated model in order to:
  - Be able to continually re-evaluate their security in a changing (adversarial) environment
  - Better prepare for disruptions
  - Evaluate different approaches to mission assurance.
- Our team is creating a framework to model actual port operations and to simulate cascading disruptions and compute economic impact.
- Goal is to build a theoretically-sound tool of practical value for evaluating cascading disruptions left, center, and right of boom.
Thank You!

- USTRANSCOM
- Department of Homeland Security
- Information Trust Institute
- US Coast Guard
  - USCG Sector Miami
  - USCG Research & Development Center
- Port Everglades
  - Broward Country Sheriff’s Office
  - Customs and Border Protection
  - Crowley
  - Florida East Coast Railway
<table>
<thead>
<tr>
<th>Research Objectives</th>
<th>Model Port Operations</th>
<th>Catalog Disruptions</th>
<th>Cascading Effects/Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reusable, artificial but realistic cyber-physical dependency models.</td>
<td>• Type system enables one to apply disruptions to different sector dependency models [Ekelhart 2015].</td>
<td>Extend port simulation studies with cyber dependencies [Dragovic 2017].</td>
<td>Extend port simulation studies with cyber dependencies [Dragovic 2017].</td>
</tr>
<tr>
<td>Combines graph-theory with a type system to develop a language for critical infrastructure sector dependencies [Weaver et al. 2013].</td>
<td>• General disruptions may be applied to specific ports via ontologies.</td>
<td>Rank cyber-originating disruptions and their physical impacts using Monte Carlo simulation, MDO techniques, and numerical methods (DES).</td>
<td>Rank cyber-originating disruptions and their physical impacts using Monte Carlo simulation, MDO techniques, and numerical methods (DES).</td>
</tr>
<tr>
<td>Facilitate comparison and reuse [Stodden]</td>
<td>• Extend port simulation studies with cyber dependencies [Dragovic 2017].</td>
<td>Find least-cost resource allocation and mitigation strategies using an Optimal Network Flow (ONF) model.</td>
<td>Find least-cost resource allocation and mitigation strategies using an Optimal Network Flow (ONF) model.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anticipated Outputs</td>
<td>Cyber-physical injects for AMSC exercises/training.</td>
<td>Engine to rank cyber-originating disruptions to the MTS, identify cyber Single Points of Failure (SPF), etc.</td>
<td>Engine to rank cyber-originating disruptions to the MTS, identify cyber Single Points of Failure (SPF), etc.</td>
</tr>
<tr>
<td>Simple, usable models of cyber-physical dependencies [USTC]</td>
<td>• Informed by DHS THIRA [Harvill-PEV], NIST CF [Wieland-USCG], MSRAM [Regan-USCG], and others [USTC, POAL]</td>
<td>Powerful, intuitive visualizations to facilitate decision making.</td>
<td>Powerful, intuitive visualizations to facilitate decision making.</td>
</tr>
<tr>
<td>Refactor/recompose model primitives for different ports [USCG].</td>
<td></td>
<td>Useful for AMSCs to conduct risk assessment in cyber-domain prior to, during and before an incident.</td>
<td>Useful for AMSCs to conduct risk assessment in cyber-domain prior to, during and before an incident.</td>
</tr>
</tbody>
</table>