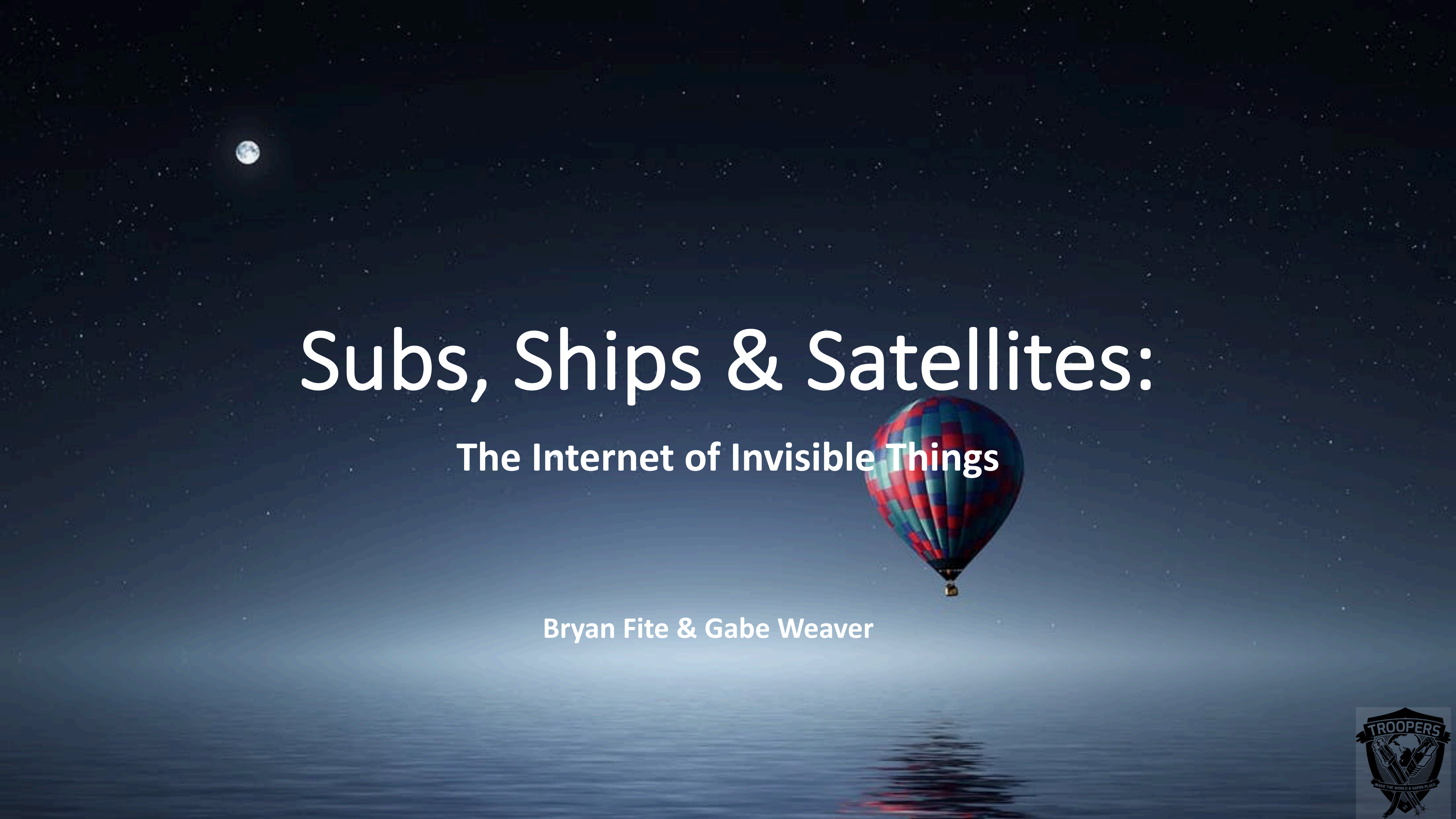


Subs, Ships & Satellites:

The Internet of Invisible Things

Bryan Fite & Gabe Weaver

Who R We?

Longing for interdisciplinary research…
@polutroposter

The guy that used to say NO and now facilitates YES

@BryanFite

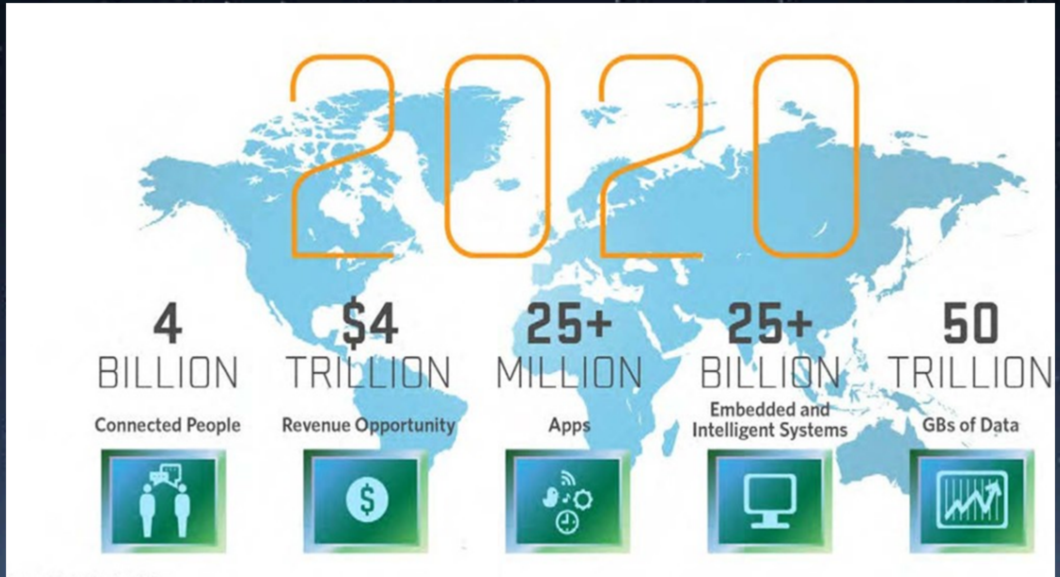
WORLDS ARE COLLIDING
quickmeme.com

HUMAN

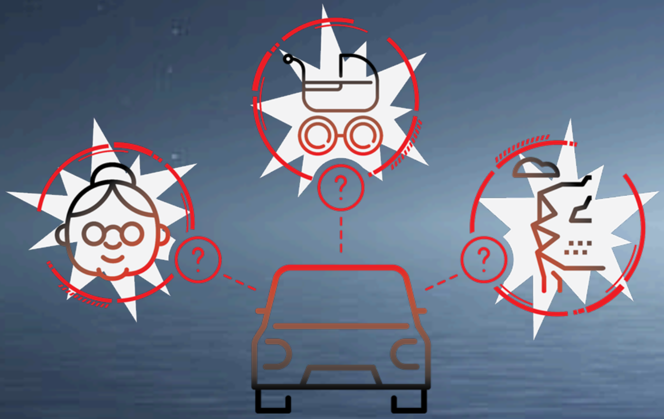
HUMANS MATTER

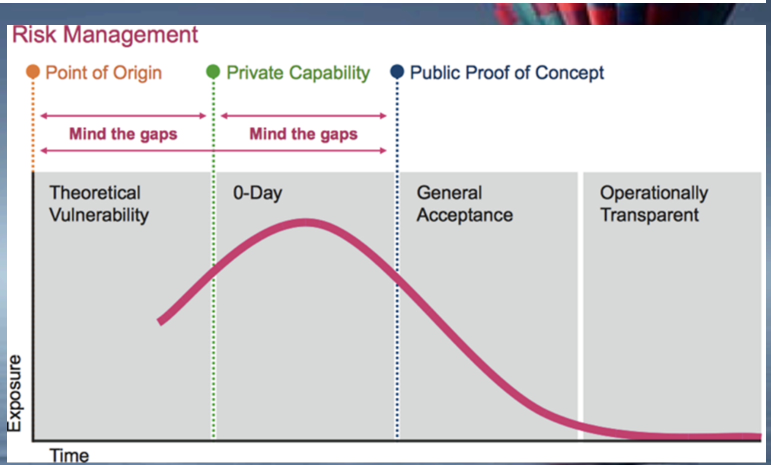
What’s your Exposure Index?

EI = Motivation * Capability * Vulnerability



Source: Mario Morales, IDC



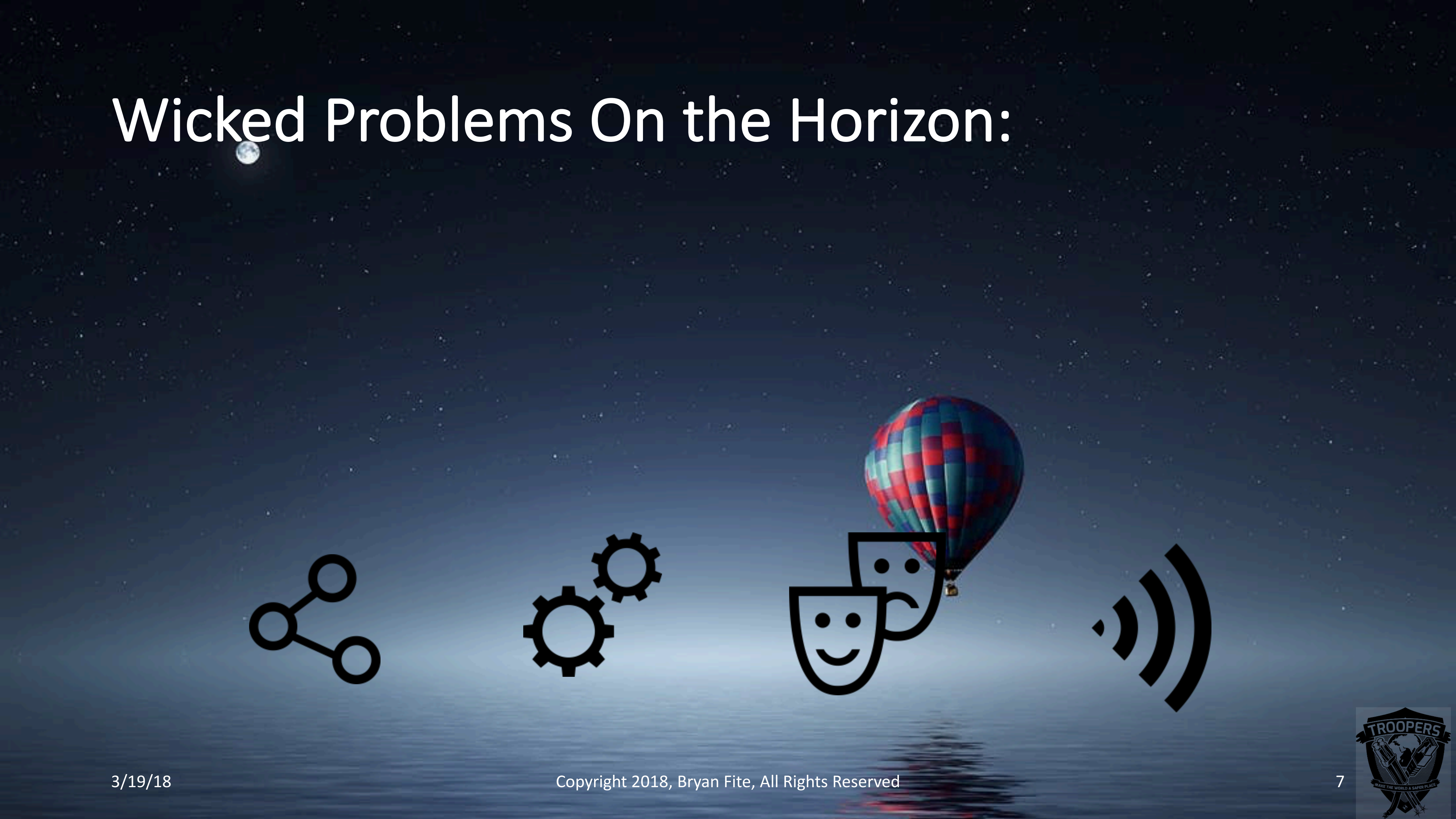


But wait there's more…"What you can't see can hurt you!"

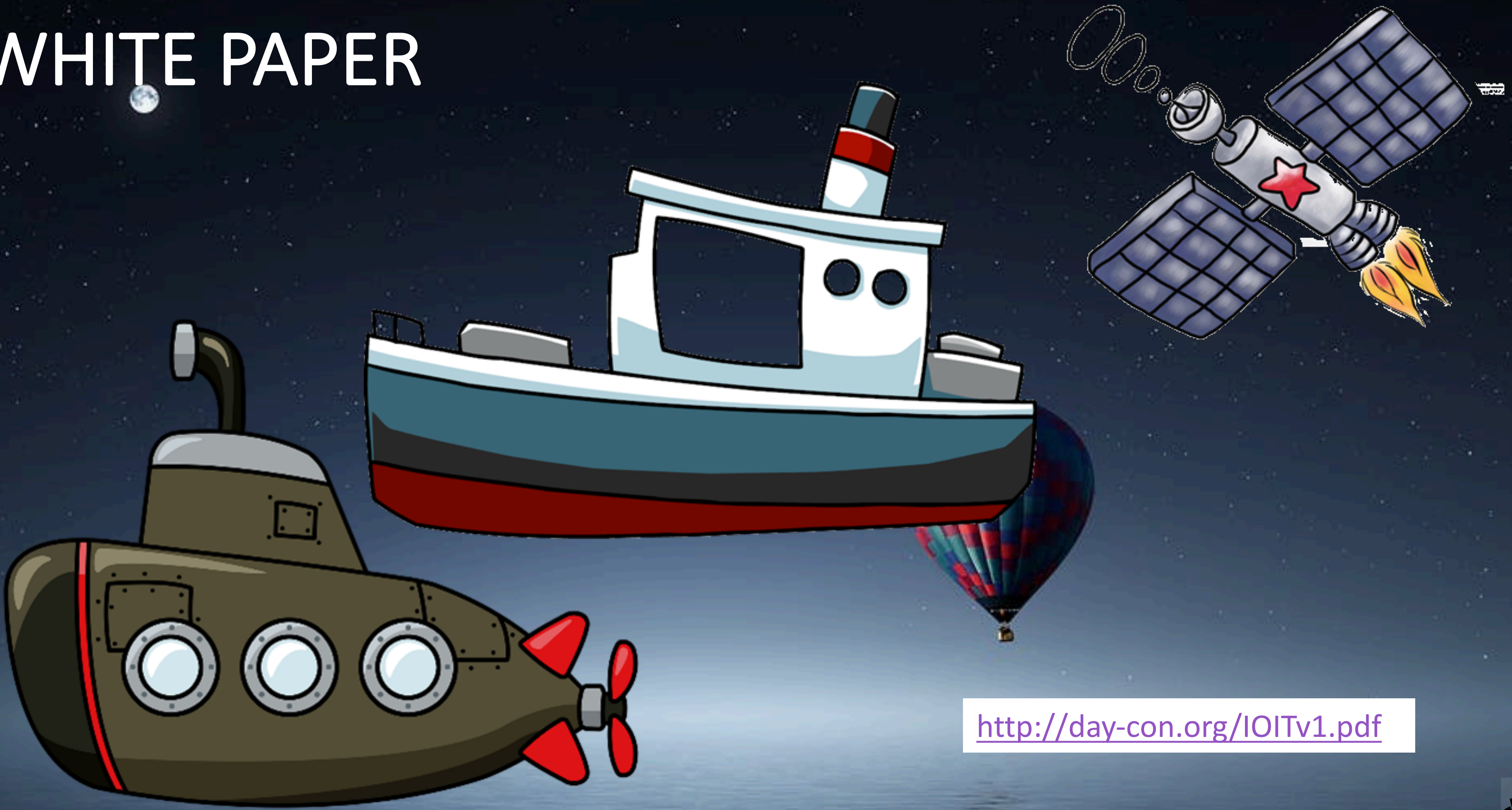
A SIRIUS CYBERNETICS CORPORATION PRODUCT
S.E.P 2000
SOMEONE ELSE'S PROBLEM FIELD GENERATOR
GUIDE APPROVED!
S.E.P 2000
BATTERY INCLUDED:
EST. BATTERY LIFE 100+ YEARS
FREE TOWEL WITH
EVERY PURCHASE
shirtoid.com

The Internet of Invisible Things

Wicked Problems On the Horizon:

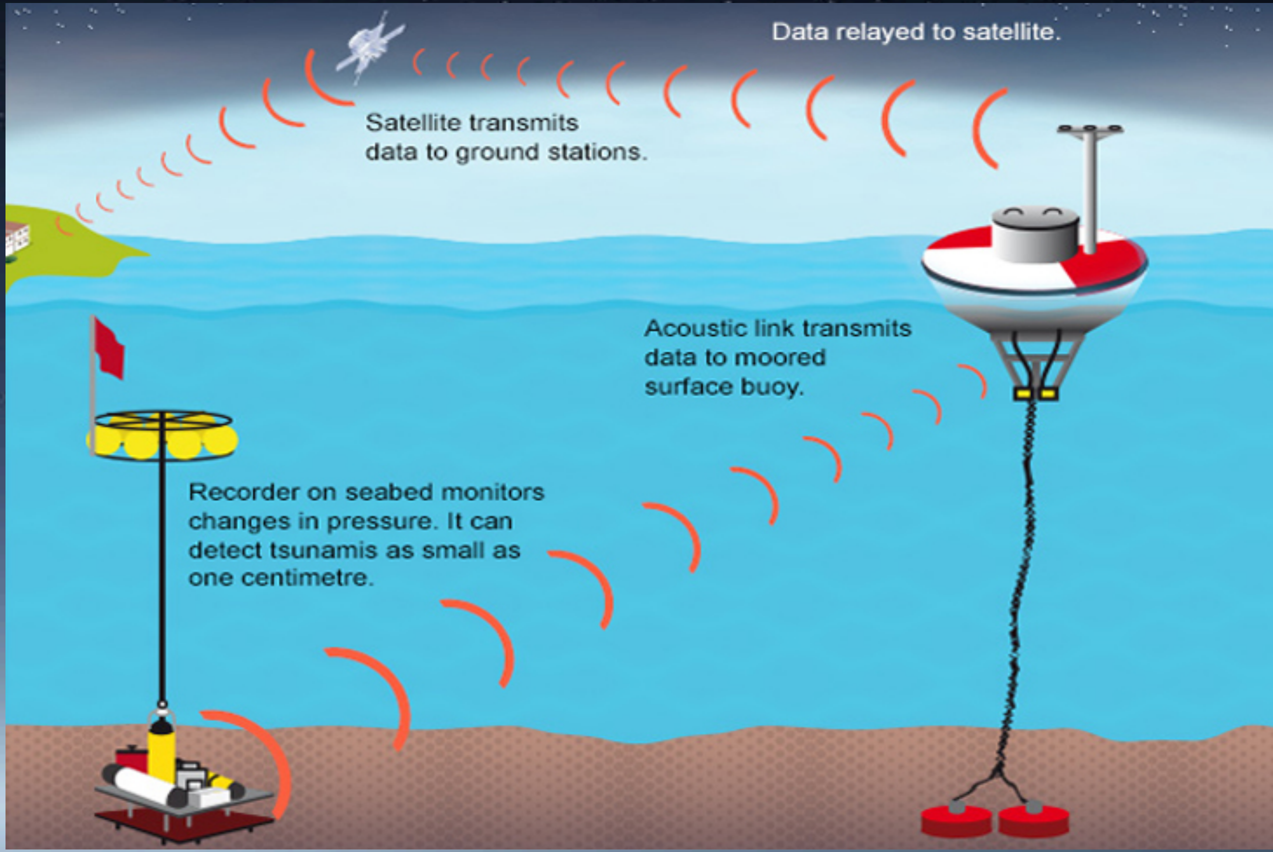


WHITE PAPER



http://day-con.org/IOITv1.pdf

Tsunami Warning System


Data relayed to satellite.
Satellite transmits data to ground stations.
Acoustic link transmits data to moored surface buoy.
Recorder on seabed monitors changes in pressure. It can detect tsunamis as small as one centimetre.

Deep Dive

Assessment and Measurement of Port Disruptions

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
RS21
THERE'S A SMARTER WAY
HEARTLAND
Science & Technology Group
START

Select a Shipping Port

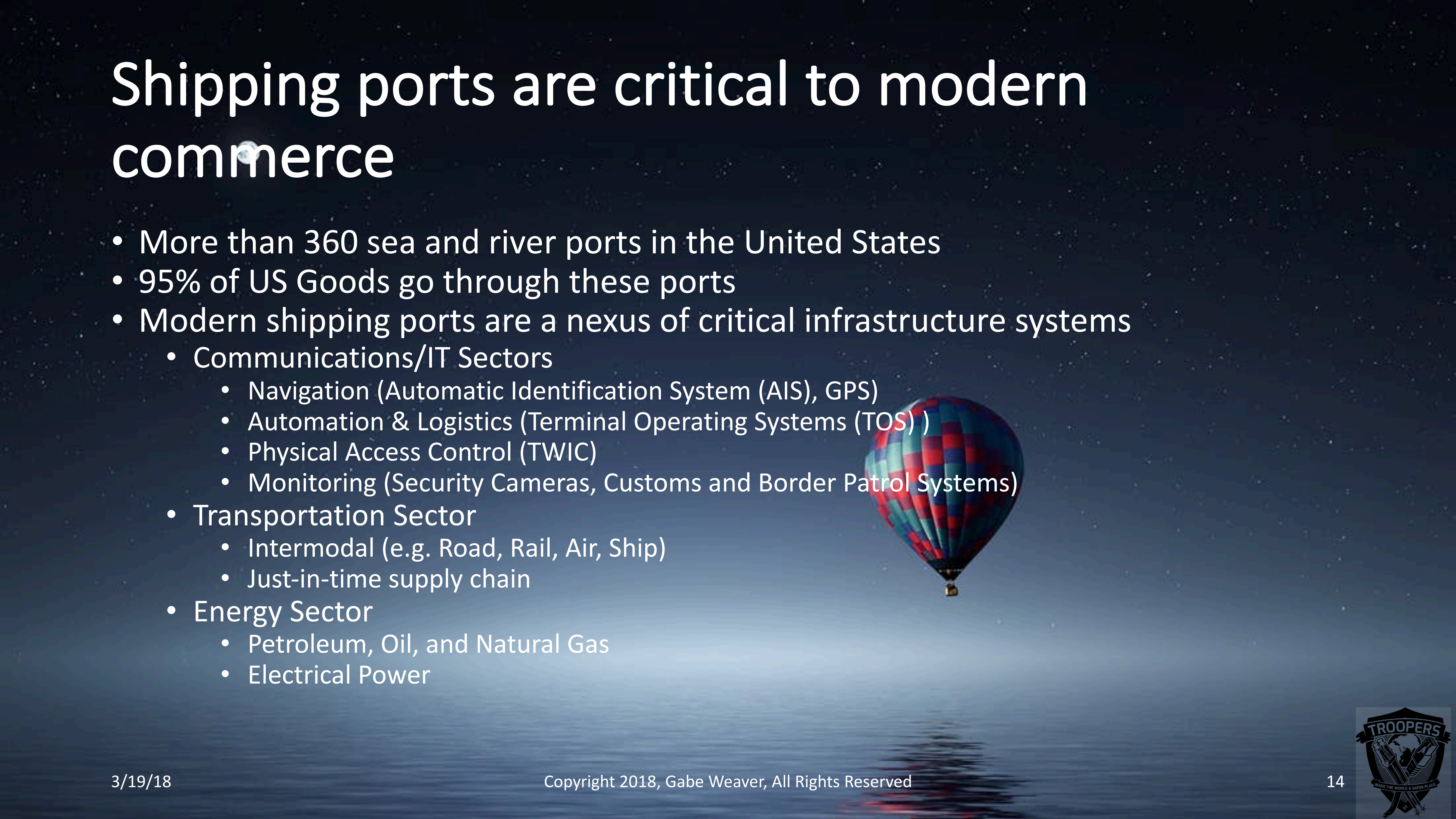
Port Everglades, FL

Ports of Auckland, NZ

Port Everglades, FL

Shipping ports are critical to modern commerce

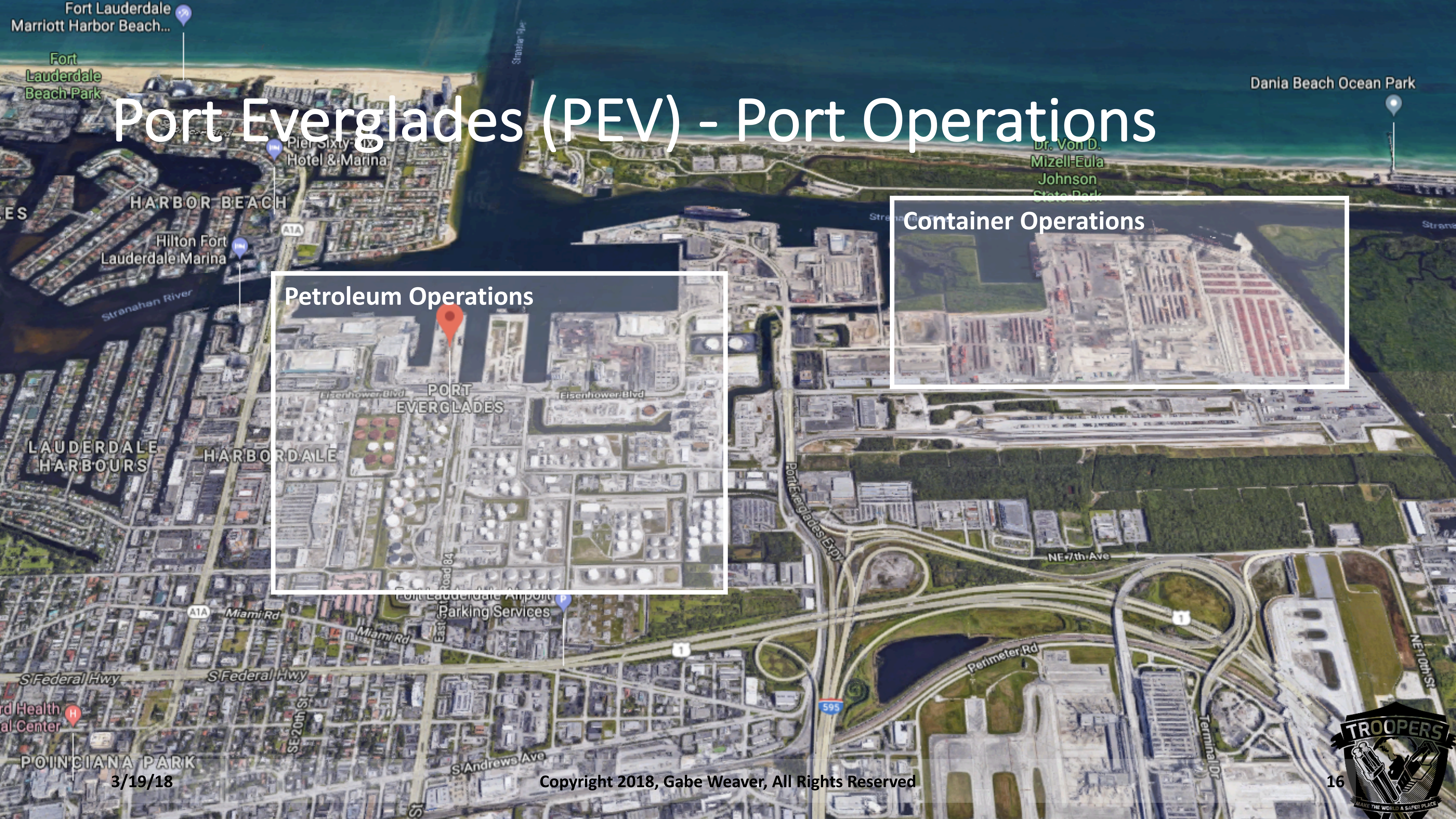
- More than 360 sea and river ports in the United States
- 95% of US Goods go through these ports
- Modern shipping ports are a nexus of critical infrastructure systems
  - Communications/IT Sectors
    - Navigation (Automatic Identification System (AIS), GPS)
    - Automation & Logistics (Terminal Operating 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



Port Operations

Fieldwork outside of the Ivory Tower

Port Everglades (PEV) - Port Operations



Petroleum Operations

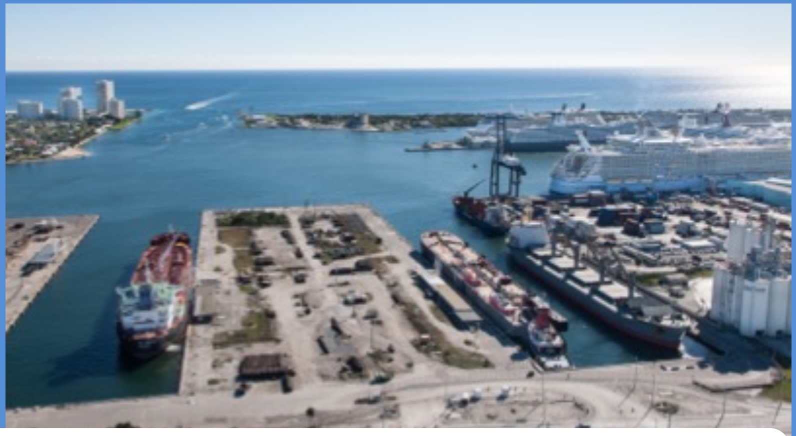
Container Operations

Pev - Petroleum Operations

1

Petroleum Pier

Tankers carrying gasoline, jet fuel, and other bulk liquids dock at the terminal.



5

Access Road

Trucks move in and out of the port via access roads.

4

Load Rack

At the load rack, trucks get the right blend and amount of gasoline.

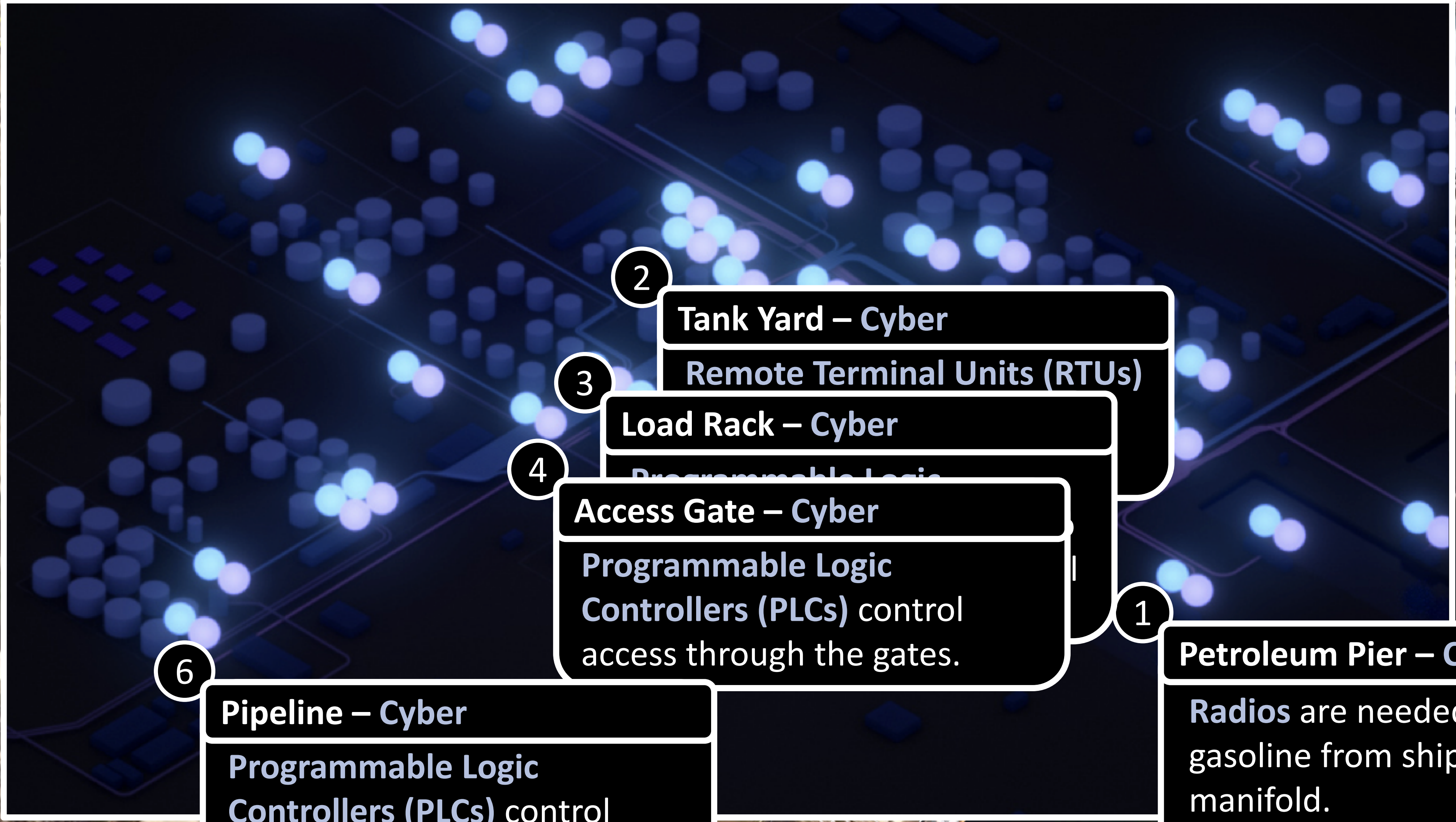
2

Tank Yard

Products are pumped through the manifold and are stored in large tanks.

t fuel
ng

BENEATH THE SURFACE: PETROLEUM OPERATIONS



1

Petroleum Pier – Cyber

Radios are needed to pump gasoline from ship to the fuel manifold.

2

Tank Yard – Cyber

Remote Terminal Units (RTUs)

3

Load Rack – Cyber

Programmable Logic

4

Access Gate – Cyber

Programmable Logic Controllers (PLCs) control access through the gates.

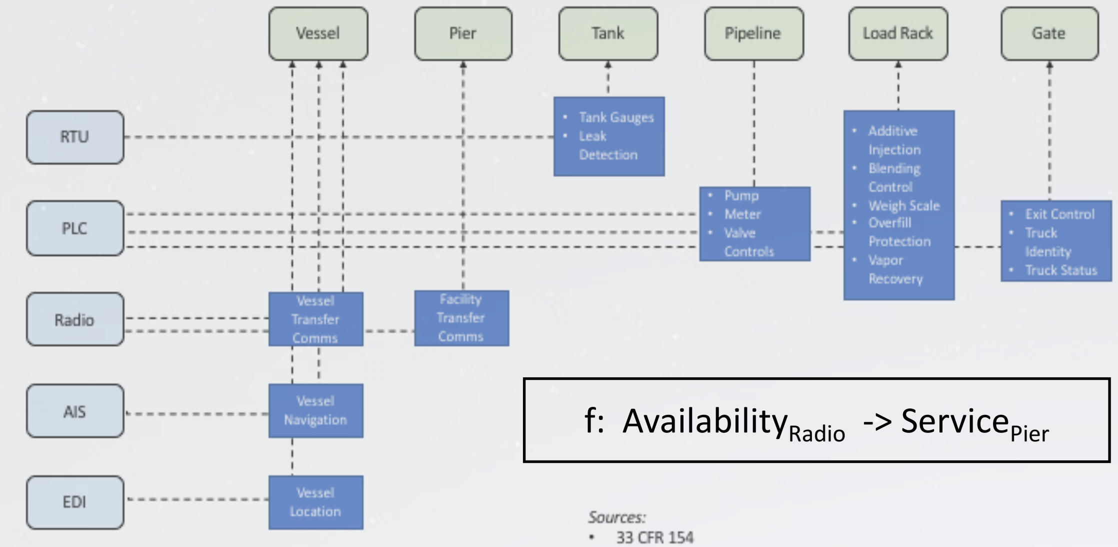
6

Pipeline – Cyber

Programmable Logic Controllers (PLCs) control pipeline meters and pumps.

Simple Example: Petroleum Operations

(G_{cyber}): Cyber network

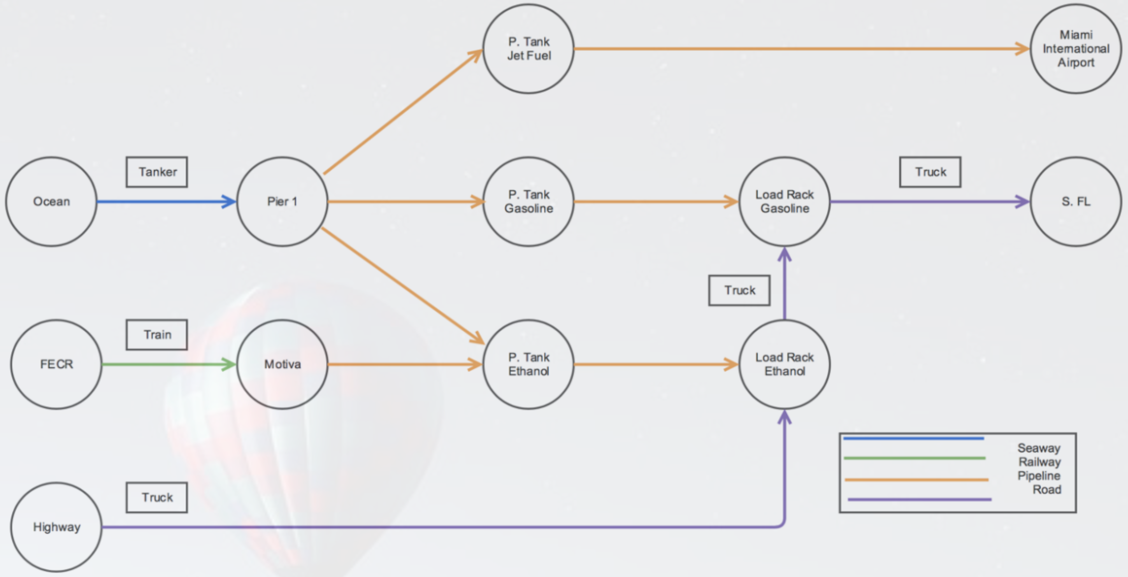


f: $\text{Availability}_{\text{Radio}}$ -> $\text{Service}_{\text{Pier}}$

Sources:

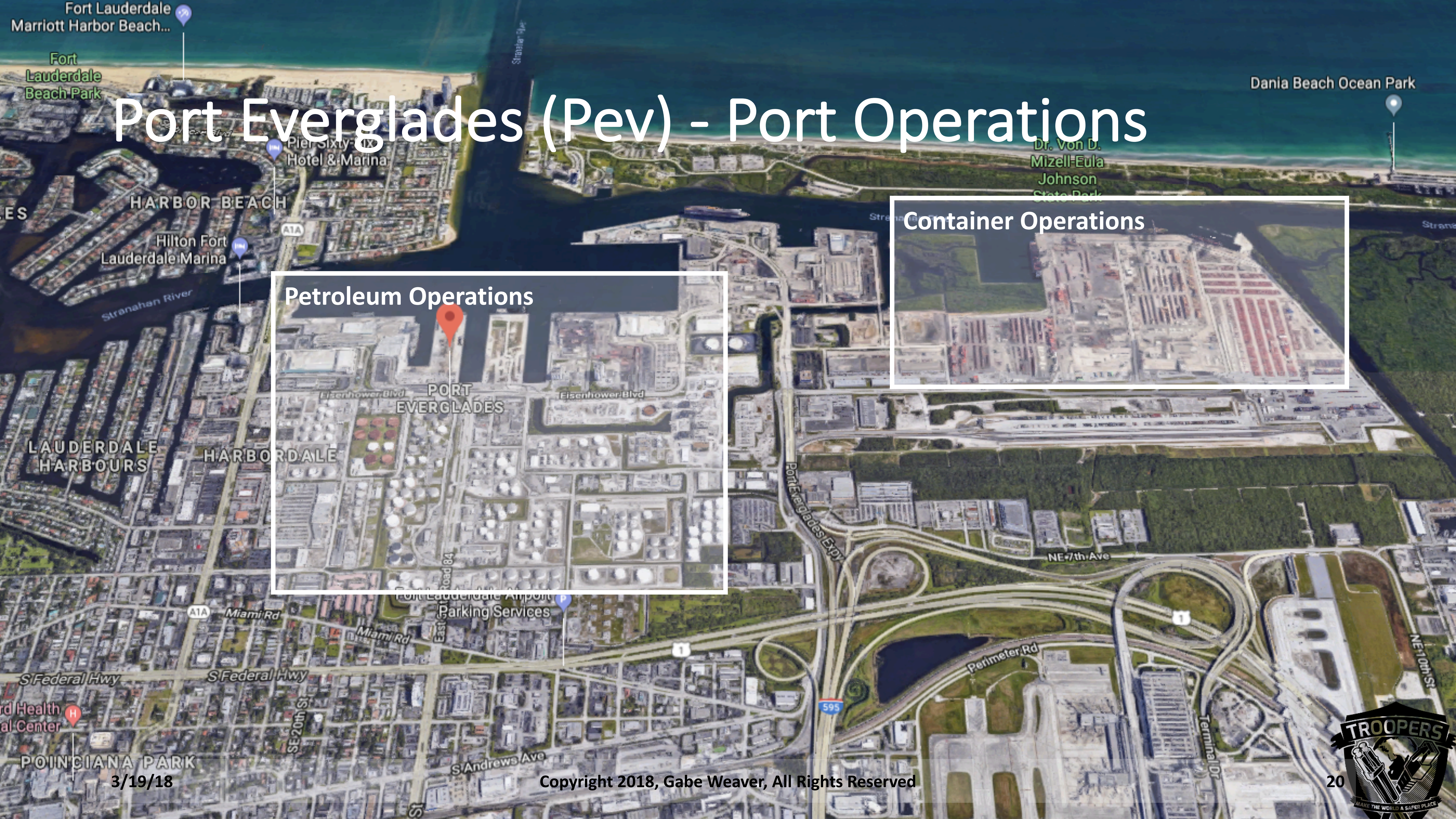
- 33 CFR 154
- http://www.varec.com/docs/pro037_terminalautomation.pdf

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



Commodity	Location	Cost
Unleaded Gasoline	Texas	0.50
	Europe	0.40
Jet/Kerosene	Texas	0.60
	Europe	0.58

Port Everglades (Pev) - Port Operations



Petroleum Operations

Container Operations

ratio

5 Seaway

Ships move in and out of the seaway in order to bring goods into (import) and out of the port (export).

4 Gantry Cranes

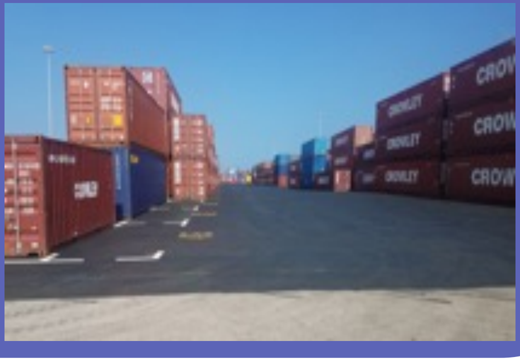
Gantry cranes load and unload cargo containers from ships docked at the terminal.

2 Gate

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

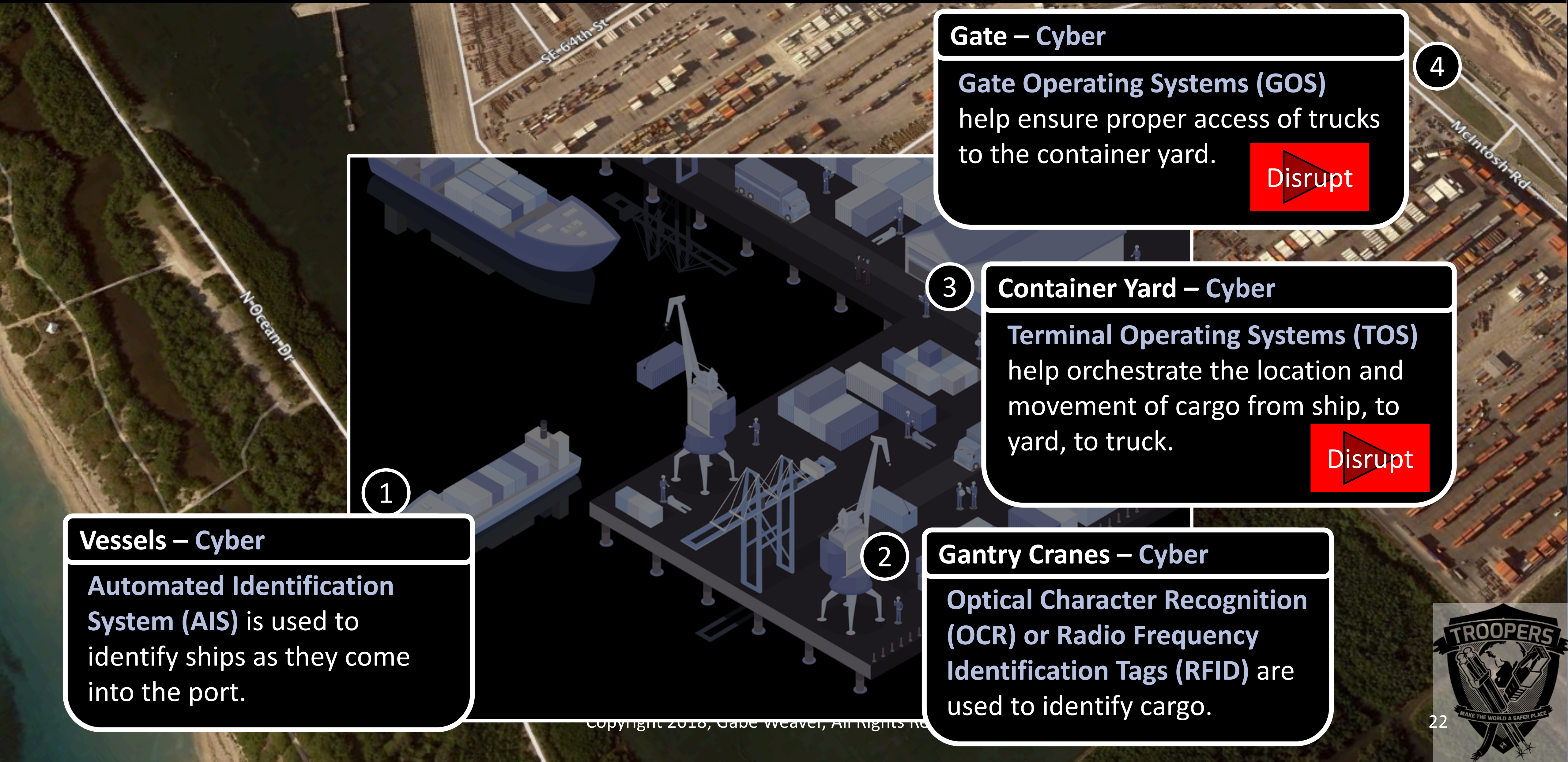
3 Container Yard

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



ey

BENEATH THE SURFACE: CONTAINER OPERATIONS



1

Vessels – Cyber

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

2

Gantry Cranes – Cyber

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

3

Container Yard – Cyber

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

Disrupt

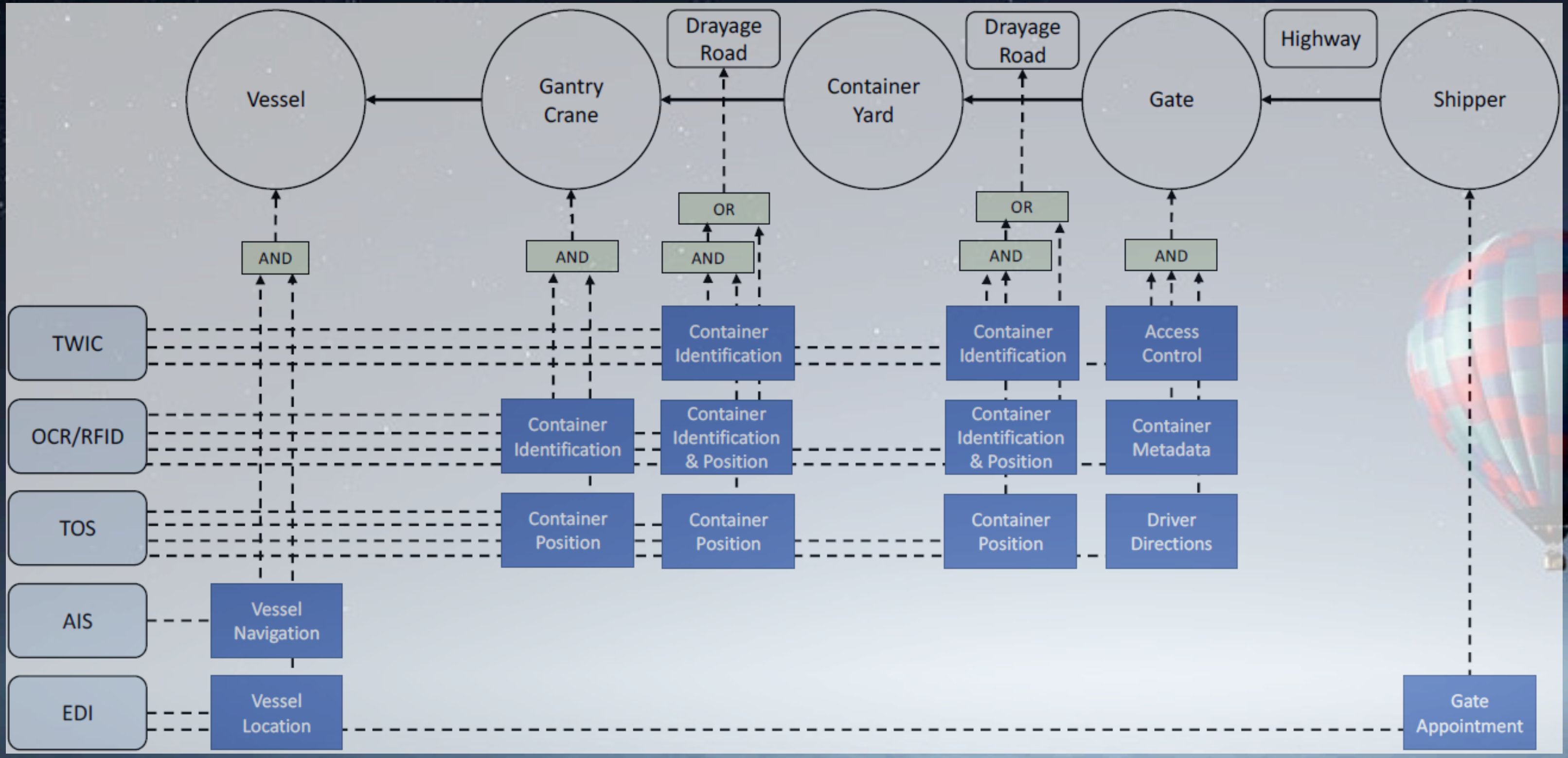
4

Gate – Cyber

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

Disrupt

Example Network: Container Cargo



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

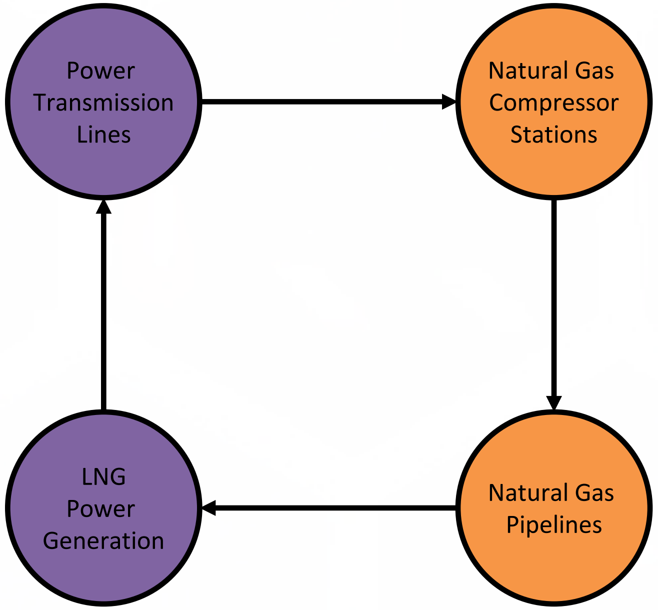
← **Pathway**
Roads : Rail: Seaway : Air : Etc.

▭ **Resource**
Gantry Crane : TWIC : Gate : Etc.

Networks
Transportation : Cyber : Power
Petroleum : Etc.

Disruptions
Delays : Restricted Routes :
Outages : Increased cost : Etc.

Network Motif



Topology Generation

Construct graphs G_{power}o G_{lng}

- Connect:
  - Generators to Transmission Lines that are *close*.
  - Transmission Lines to Stations that are *close.*
  - Stations to Pipelines that are *close.*
  - Pipelines to Generators that are *close.*

Notion of *close* is defined by geographic distance.
Data provided by HIFLD.

Network Theory/Structural Complexity

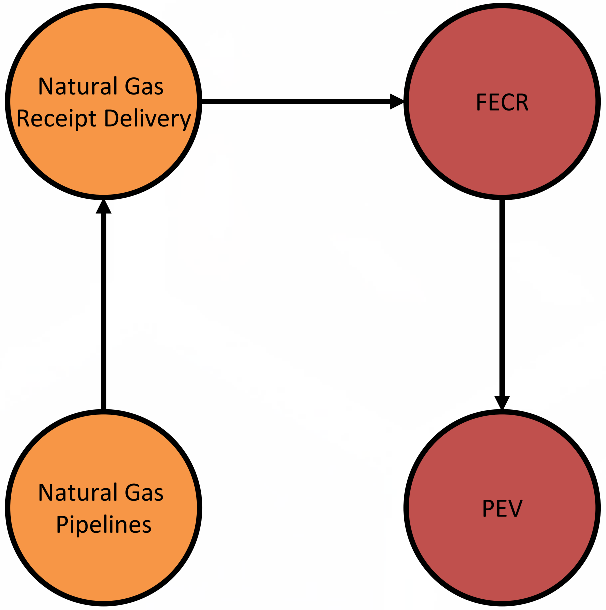
How many motifs show up within a State?

- Plot the count per State/Region.

Simulation

Co-simulation of electrical power flow (PyPSA) with liquid natural gas.

Network Motif



Topology Generation

Construct graphs $G_{power} o G_{lng}$

- Connect:
  - Generators to Transmission Lines that are *close*.
  - Transmission Lines to Stations that are *close.*
  - Stations to Pipelines that are *close.*
  - Pipelines to Generators that are *close.*

Notion of *close* is defined by geographic distance.
Data provided by HIFLD.

Network Theory/Structural Complexity

How many motifs show up within a State?

- Plot the count per State/Region.

Simulation

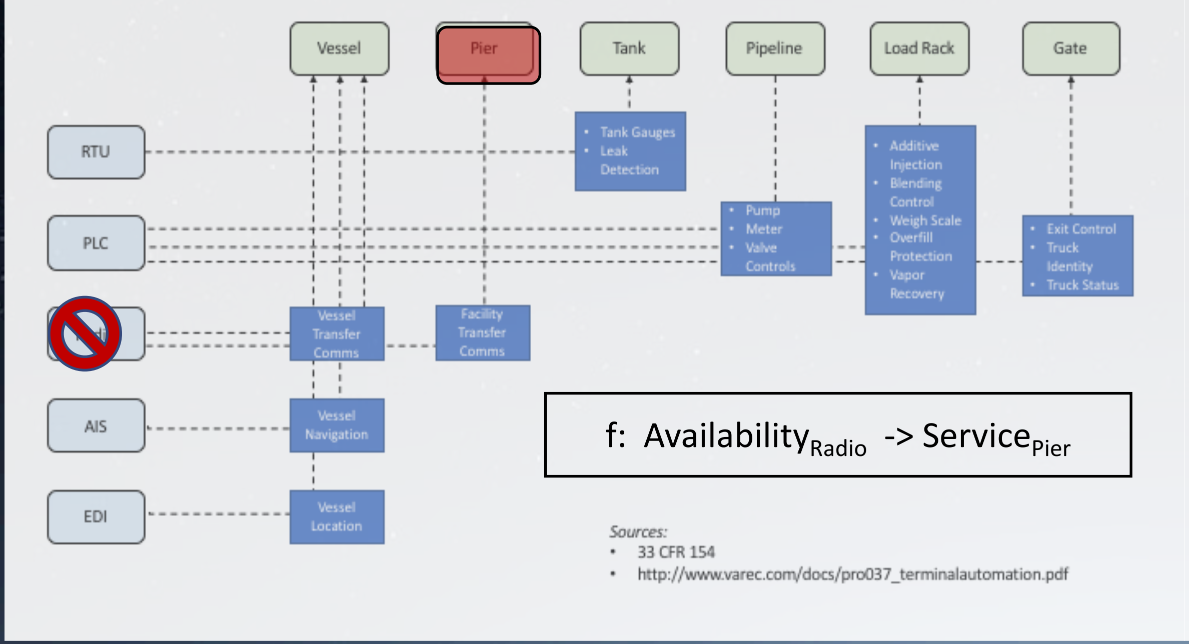
Co-simulation of Natural Gas Delivery with Railroad.

Cyber-Physical Disruptions

Simple Example Disruption

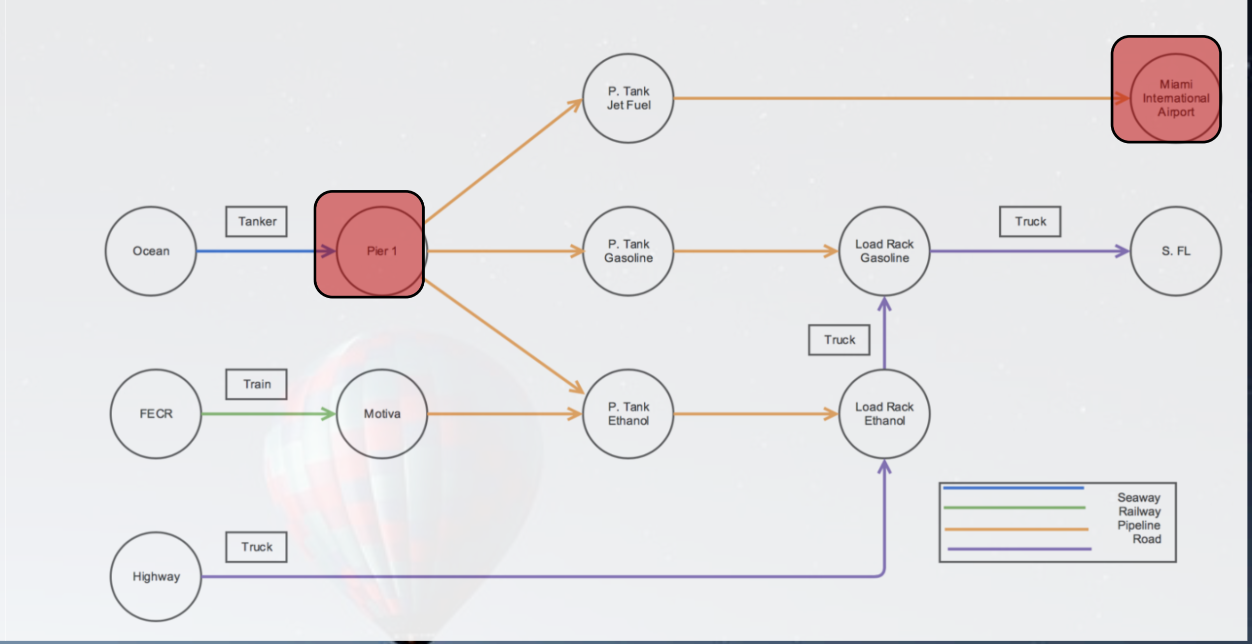
(G_{cyber}): Cyber network

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



$f\colon \text{Availability}_{\text{Radio}} \rightarrow \text{Service}_{\text{Pier}}$

Sources:
- 33 CFR 154
- http://www.varec.com/docs/pro037_terminalautomation.pdf



Commodity	Location	Cost
Unleaded Gasoline	Texas	0.50
	Europe	0.40
Jet/Kerosene	Texas	0.60
	Europe	0.58

We catalog *cyber* disruptions within the MTS.

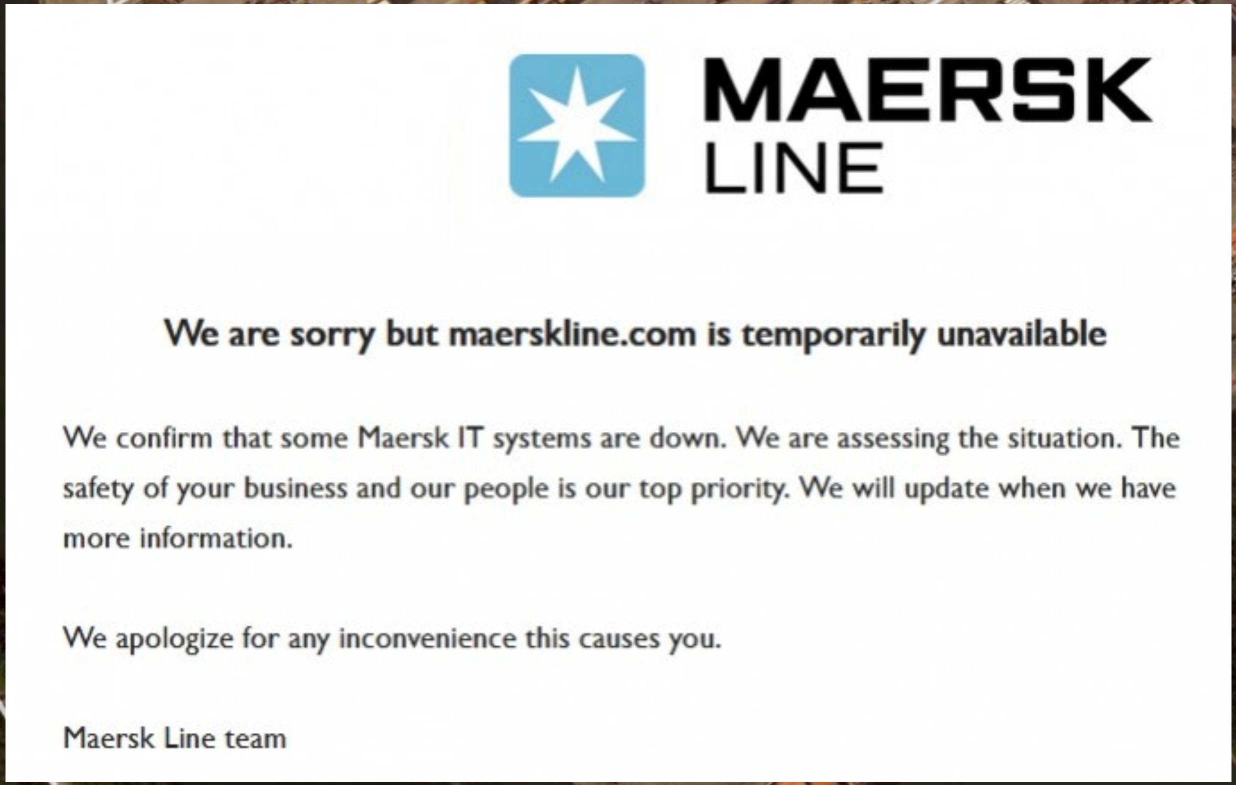
Description	Fault Category	Location	Duration	Exemplars
IT/Communications Sector				
Navigational Data (AIS, GPS)	Accidental, Intended (Nation State)	Harbormaster Tower, Quay	Hours	Somali Pirates, 2014 White Rose of Drachs, 2013
Access Control Data (TWIC)	Accidental, Intended	Port Security Gates/Terminal Operator Gates	Years	Team Digi7al Hack, 2014
Operational Data (TOS)	Accidental, Intended (Ransomware/Data Integrity/Malware)	Container Yard, Terminal Operator Gates	Days	Port of Antwerp, 2013
Monitoring Data (Security Cameras)	Accidental (Storm Surge), Intended (Hacking)	Harbormaster Tower, Security Operations Center, Security Cameras	Months	Insecam.org, Shodan Mirai (2016), Persirai (2017)
Social Engineering	Intended (Insider Attack, Phishing)	Port or Terminal Operator	Hours	Revenge sewage attacks (2001)

A Real (not Theoretical) Threat Catalog

Example scenarios for today:

1. Ransomware
2. Hacking Terminal Operations
3. GPS Jamming/Spoofing

SCENARIO 1: MAERSK *RANSOMWARE*



We are sorry but maerskline.com is temporarily unavailable

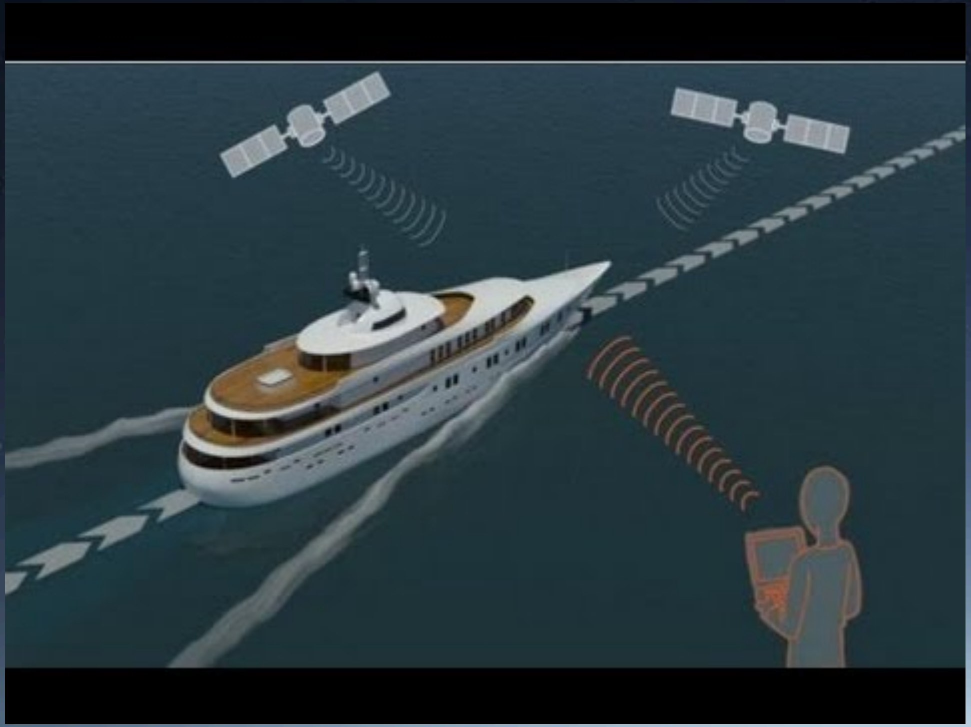
We confirm that some Maersk IT systems are down. We are assessing the situation. The safety of your business and our people is our top priority. We will update when we have more information.

We apologize for any inconvenience this causes you.

Maersk Line team

SCENARIO 2: HACKING TERMINAL OPERATING SYSTEM

Scenario 3: “Dude where’s my yacht?”



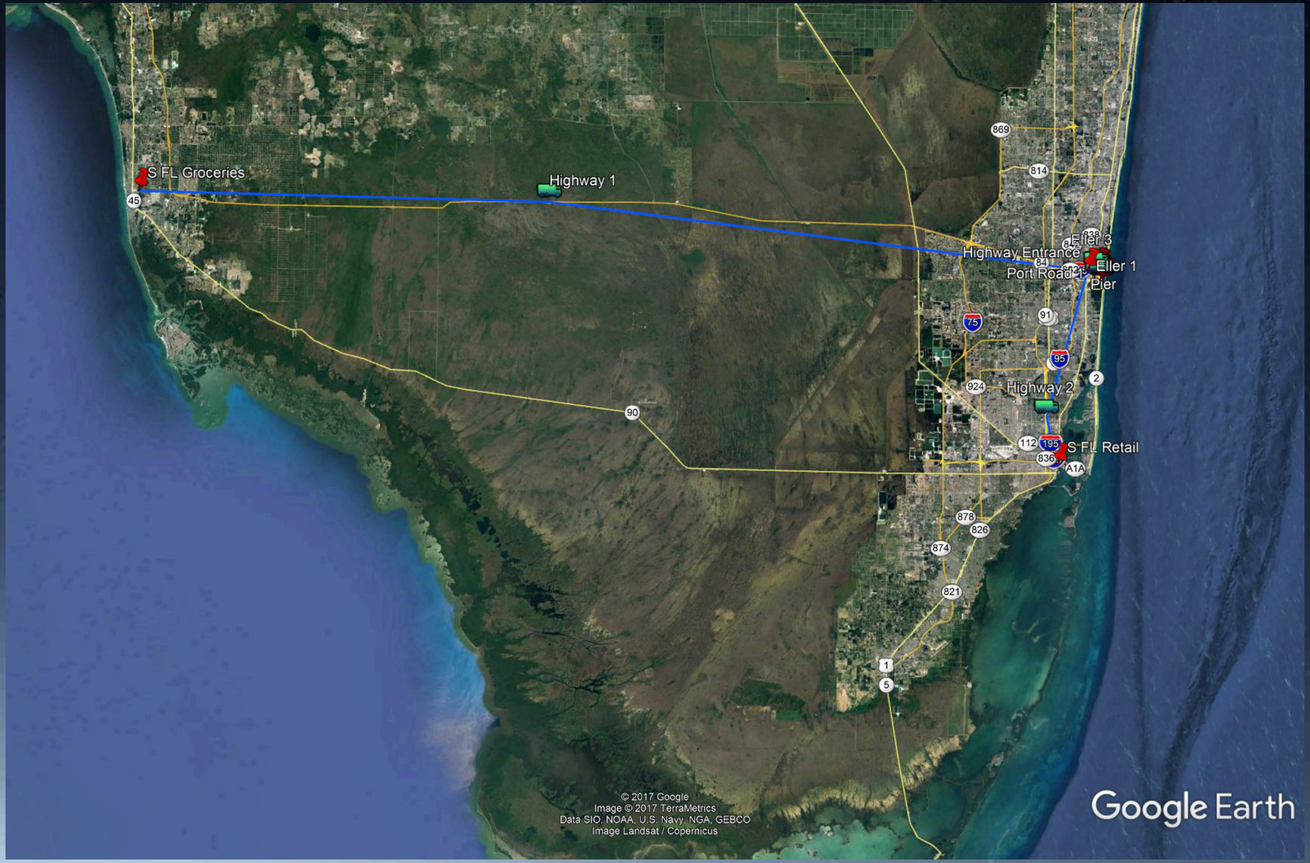
Simulation and Visualization

Packetwars™ Battle Briefing 1: Reports of Physical Control Systems going offline

- Multiple reports of sensitive physical control systems going offline coming into OC.
- Suggests a failure targeting physical access control systems.
  - TWIC
  - Gates
- Is it a systematic failure or targeted attack? (5 minutes)

Use Case

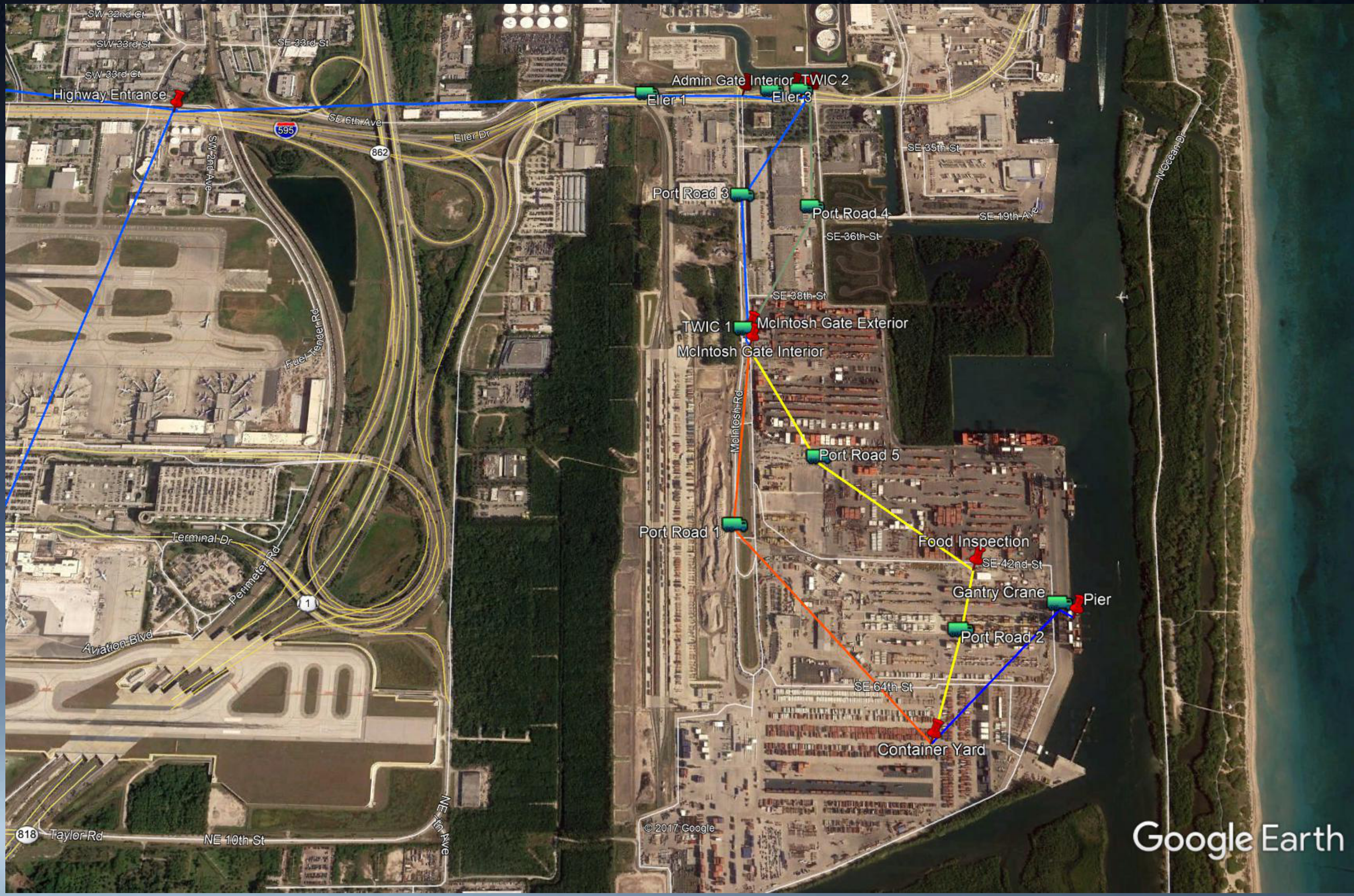
- 7 Shipments over one week
- Each shipment includes a different number of groceries and retail containers
- Cyber attack disables McIntosh gate TWIC



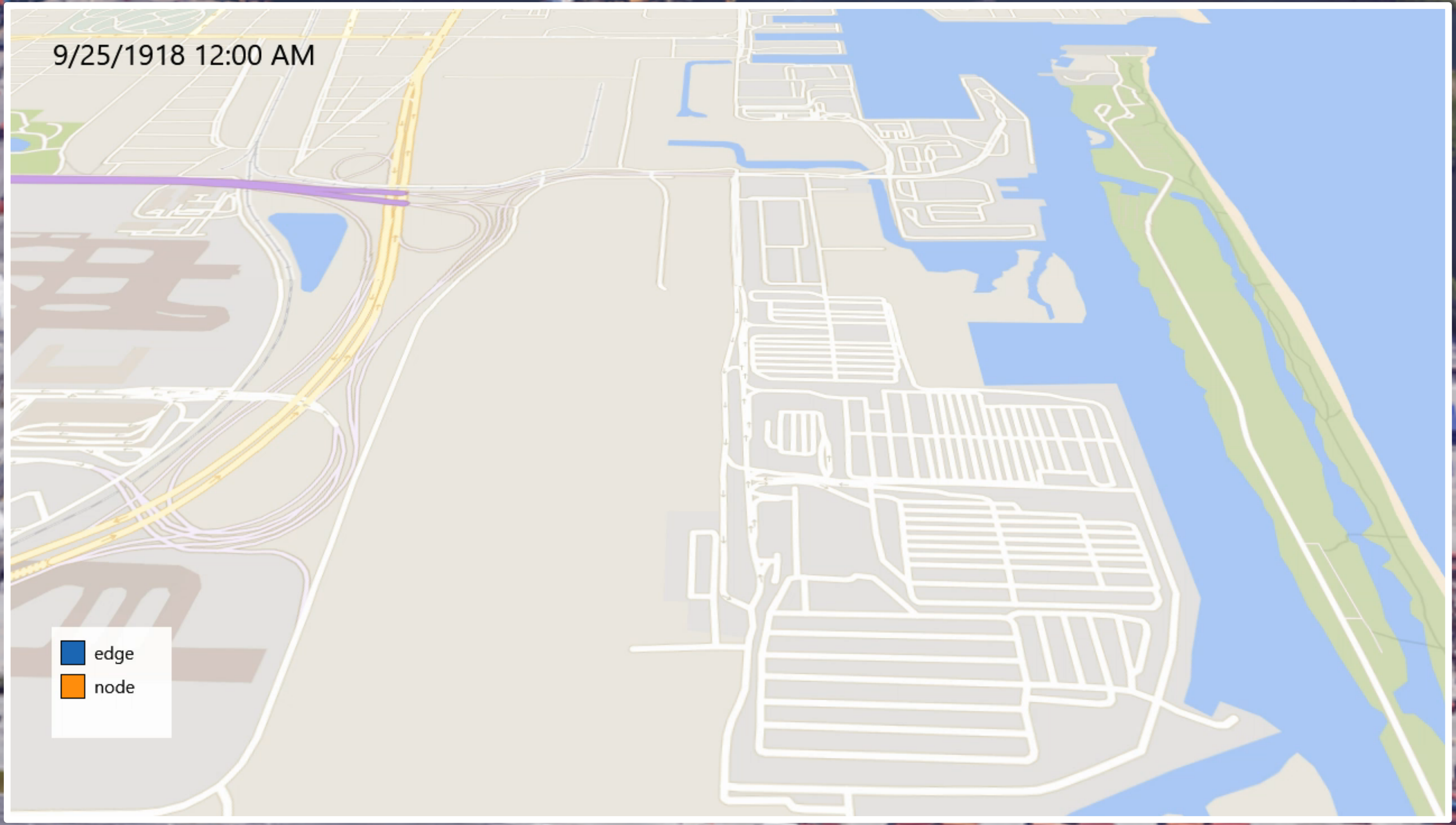
© 2017 Google
Image © 2017 TerraMetrics
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image Landsat / Copernicus

Model

- Commodities may follow different paths
- Disaster paths available
- Functional behaviors
  - Service time
  - Queue
  - Maximum throughput
  - Accumulated cost/time
  - Minimum path

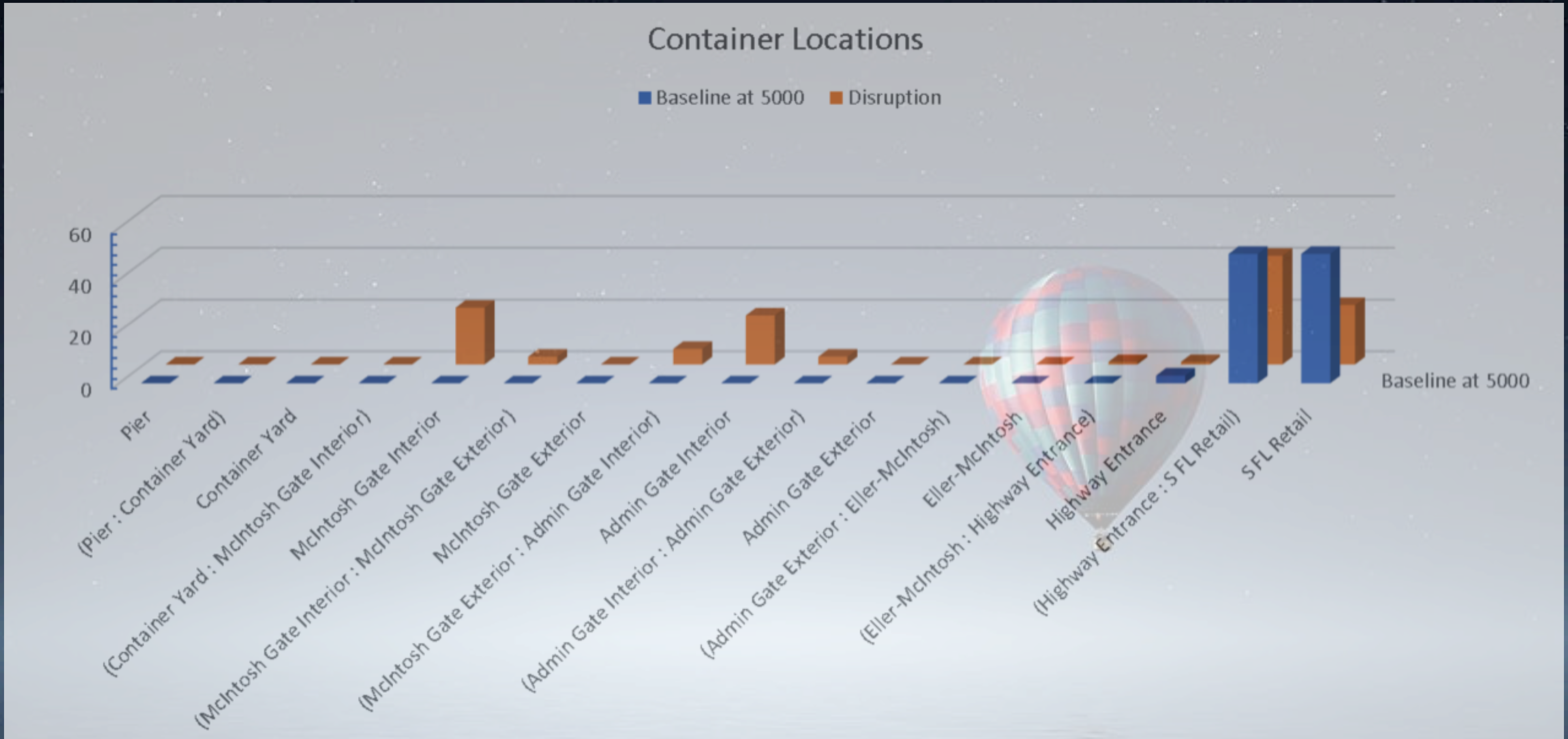


PEV - SIMULATED CONTAINER OPERATIONS



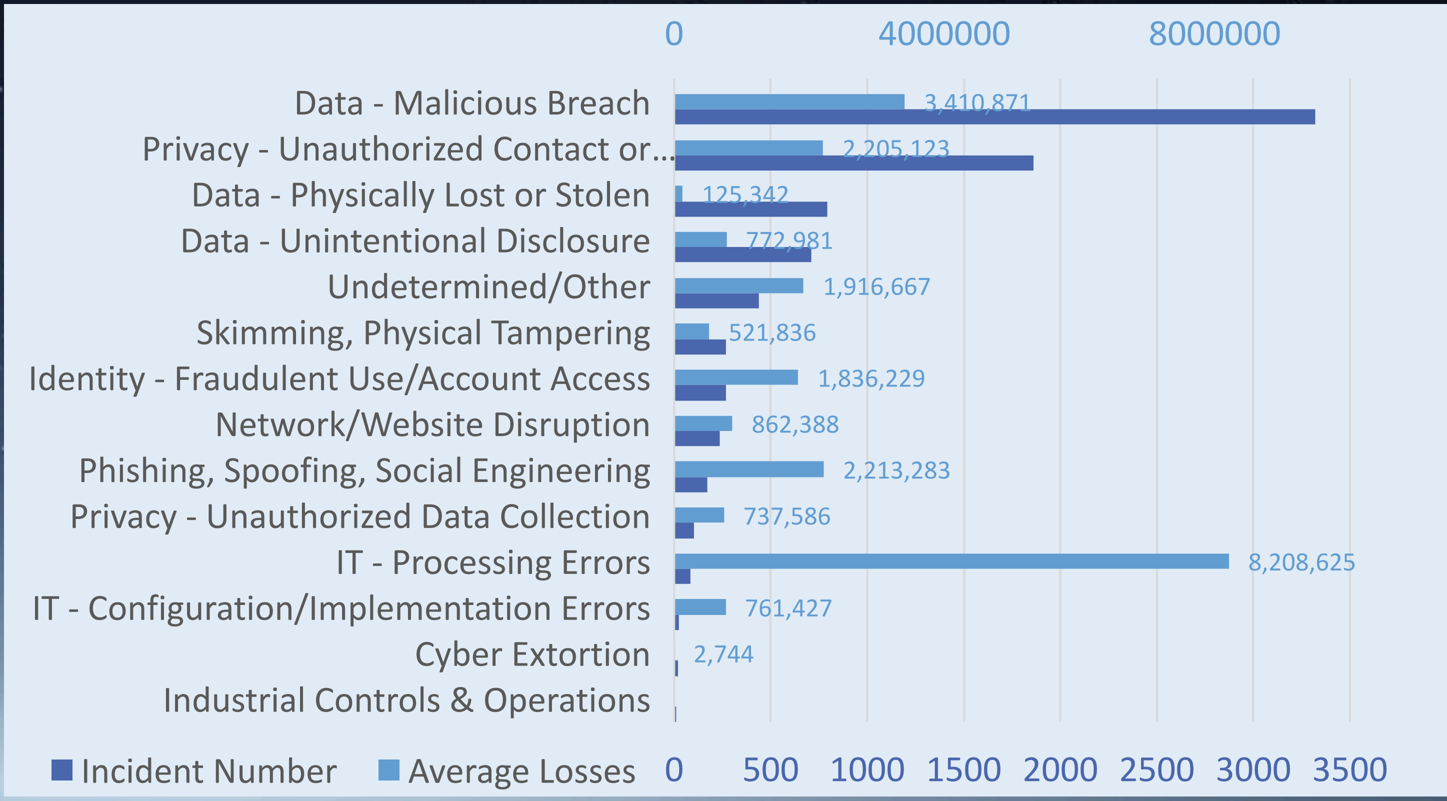
9/25/1918 12:00 AM

Disruption Effects on Retail

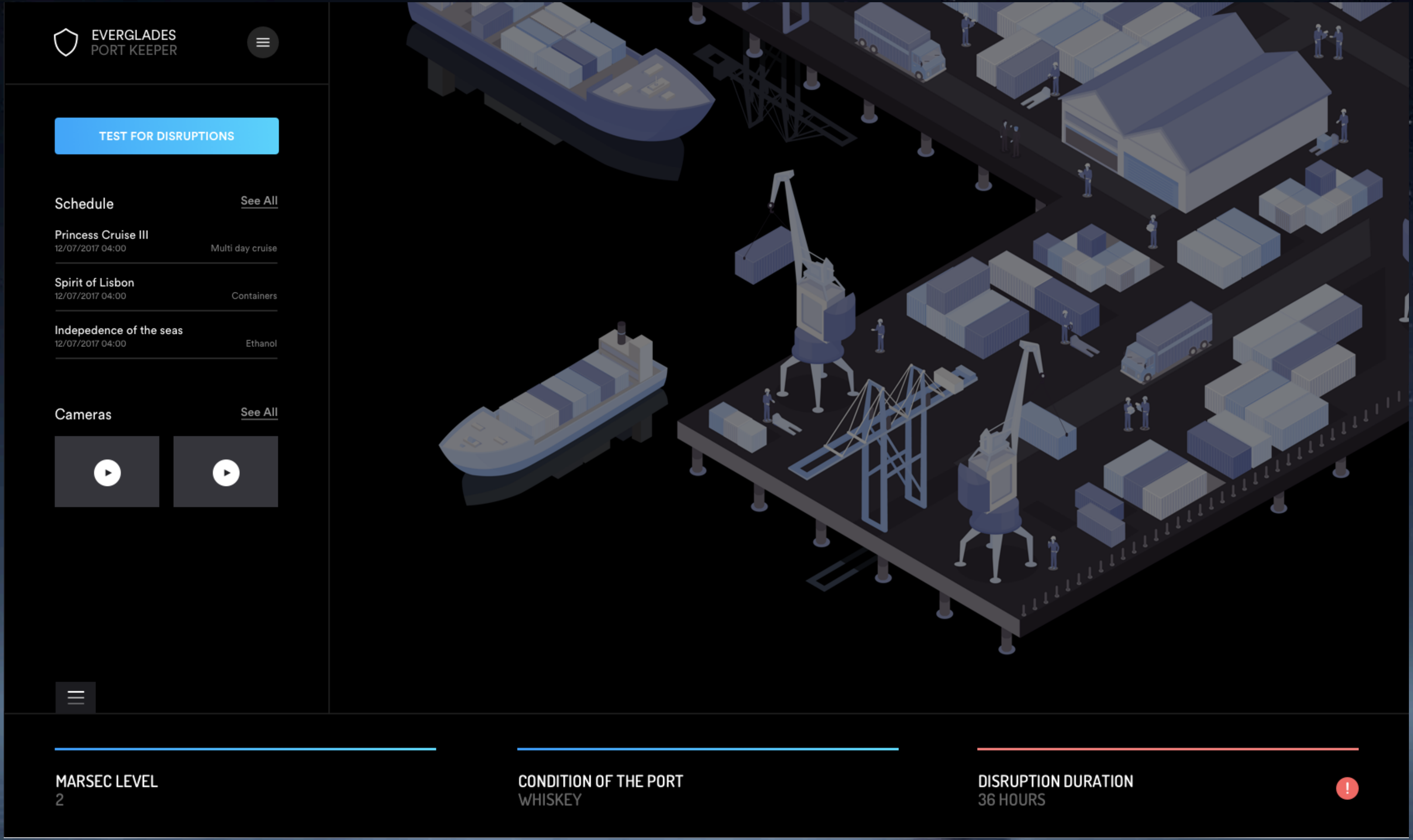


Economic Impact of Cyber Disruptions

- 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)



EVERGLADES
PORT KEEPER

Schedule

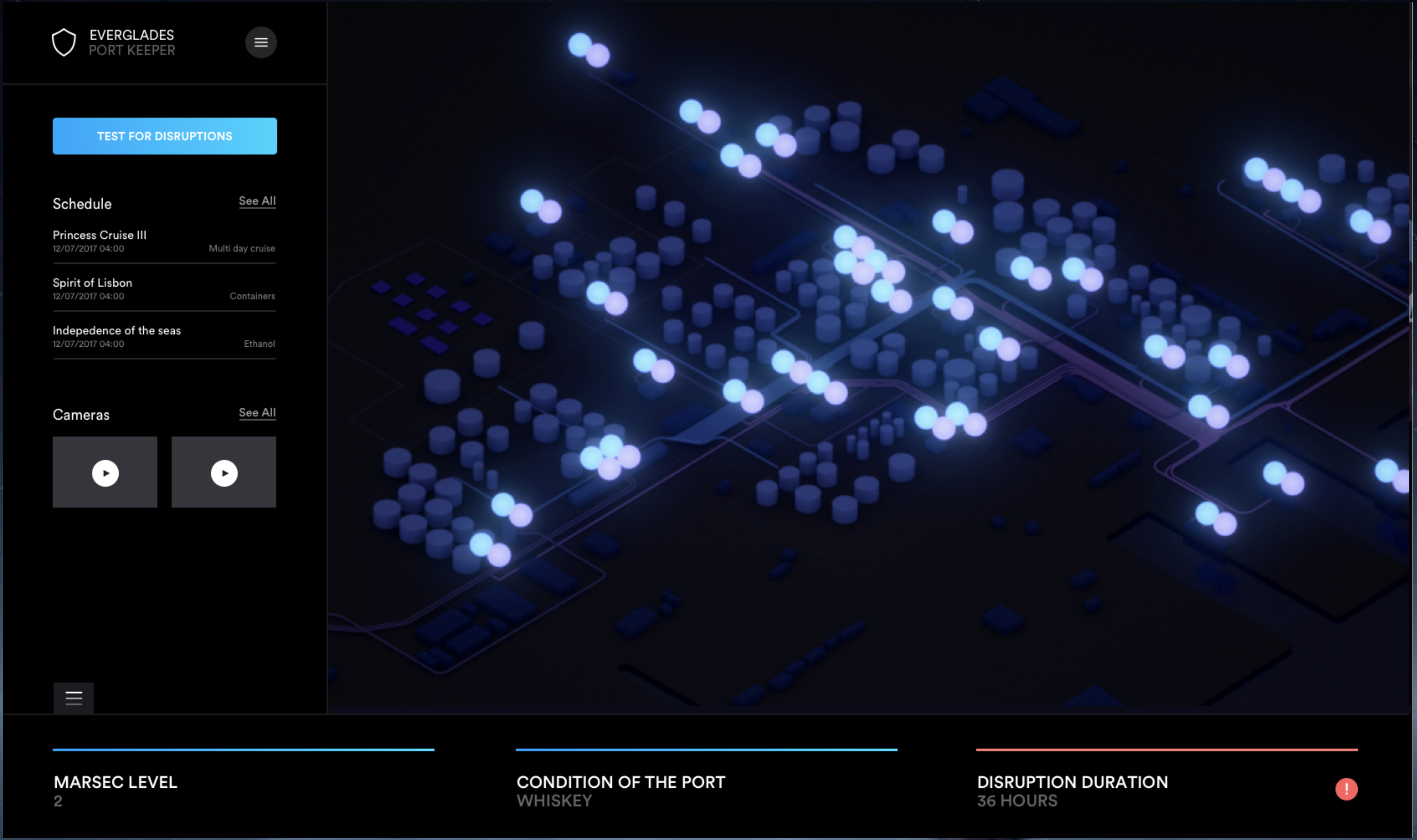
Princess Cruise III 12/07/2017 04:00	Multi day cruise
Spirit of Lisbon 12/07/2017 04:00	Containers
Indepedence of the seas 12/07/2017 04:00	Ethanol

Cameras

MARSEC LEVEL
2

CONDITION OF THE PORT
WHISKEY

DISRUPTION DURATION
36 HOURS



Schedule See All

Princess Cruise III
12/07/2017 04:00 Multi day cruise

Spirit of Lisbon
12/07/2017 04:00 Containers

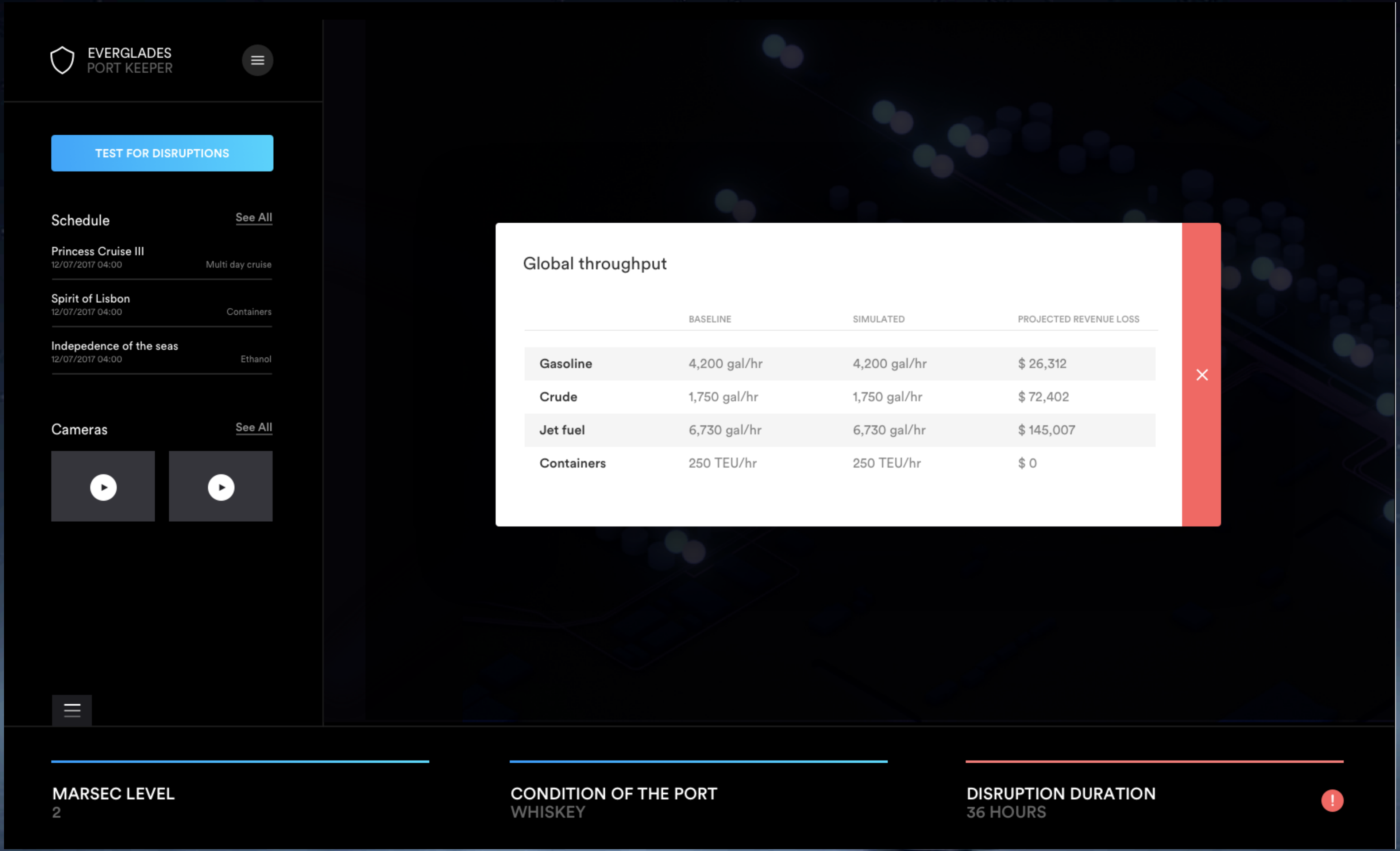
Indepedence of the seas
12/07/2017 04:00 Ethanol

Cameras See All

MARSEC LEVEL
2

CONDITION OF THE PORT
WHISKEY

DISRUPTION DURATION
36 HOURS



EVERGLADES
PORT KEEPER

TEST FOR DISRUPTIONS

Schedule See All

Princess Cruise III
12/07/2017 04:00 Multi day cruise

Spirit of Lisbon
12/07/2017 04:00 Containers

Indepedence of the seas
12/07/2017 04:00 Ethanol

Cameras See All

Global throughput

	BASELINE	SIMULATED	PROJECTED REVENUE LOSS
Gasoline	4,200 gal/hr	4,200 gal/hr	$ 26,312
Crude	1,750 gal/hr	1,750 gal/hr	$ 72,402
Jet fuel	6,730 gal/hr	6,730 gal/hr	$ 145,007
Containers	250 TEU/hr	250 TEU/hr	$ 0

MARSEC LEVEL
2

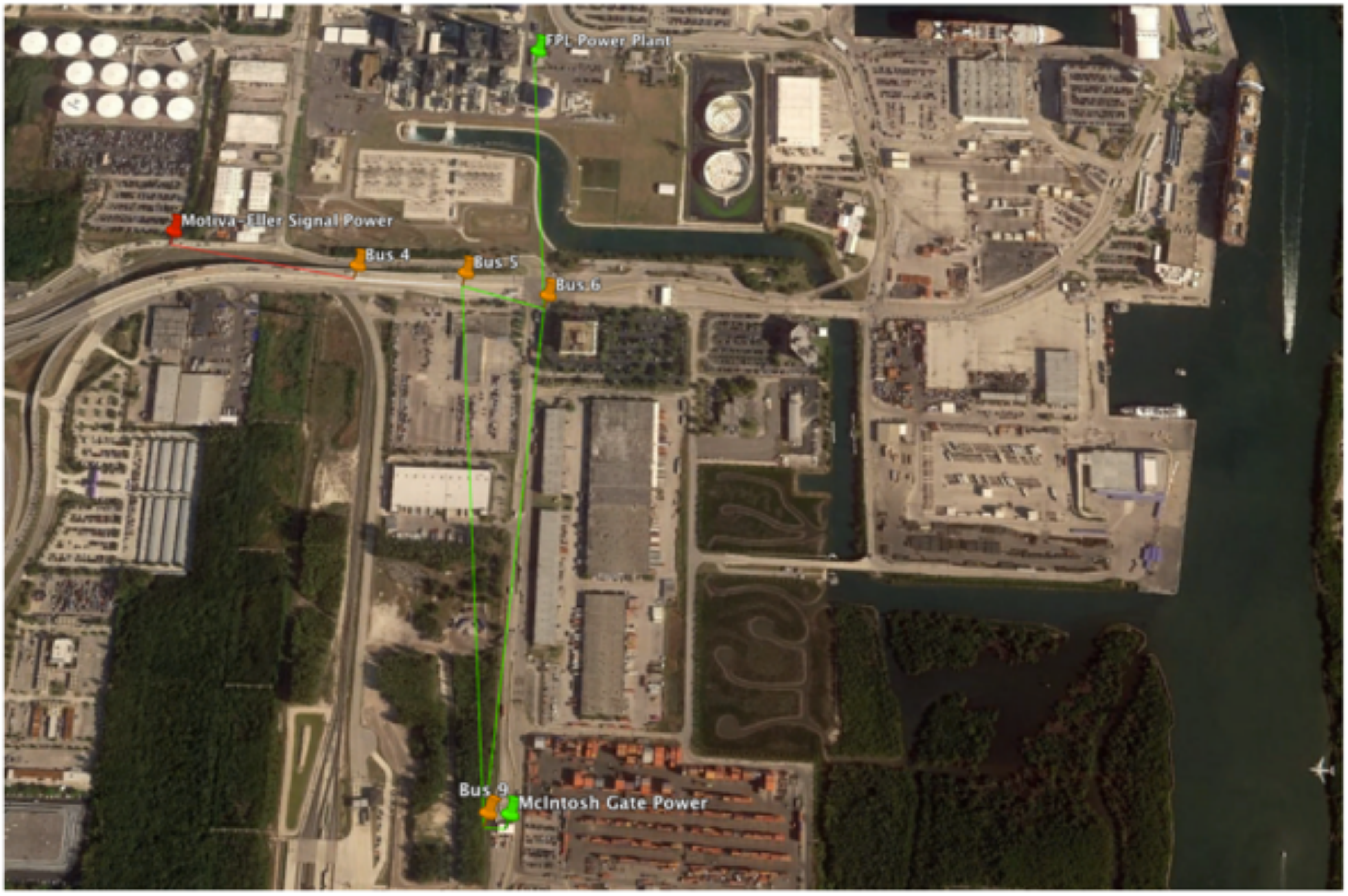
CONDITION OF THE PORT
WHISKEY

DISRUPTION DURATION
36 HOURS

Packetwars™ Battle Briefing 2: Traffic Signal

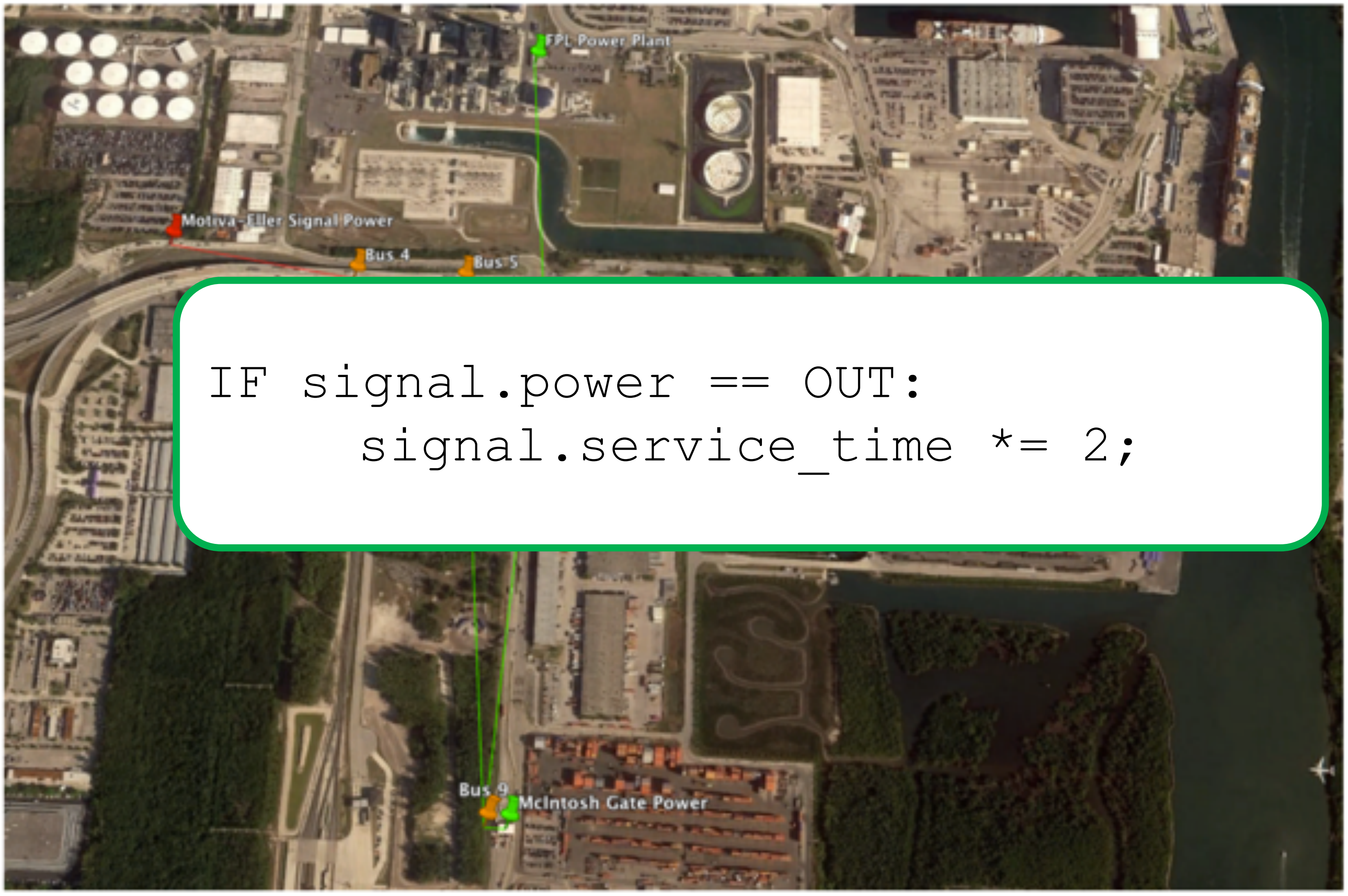
- Reports of a power outage has affected traffic signals in the port.
- The signals have battery backup but some are still failing
- What is the root cause of the outage?

Import affected assets from data source.

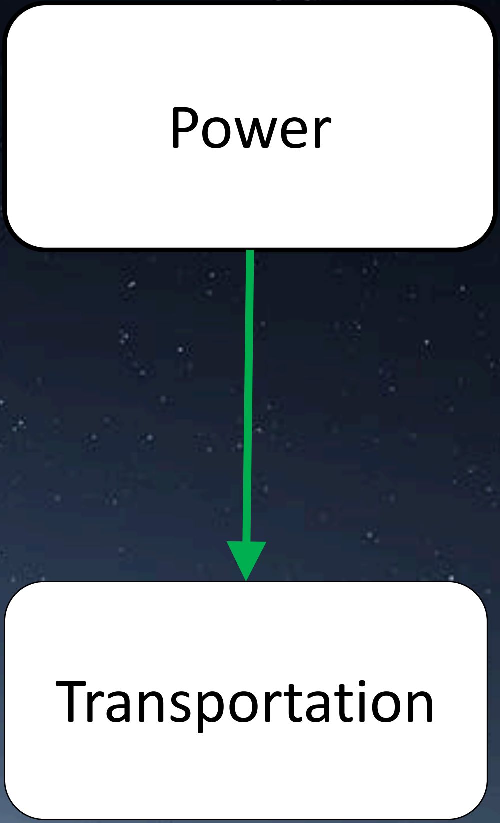


Power

Update state of transportation network.

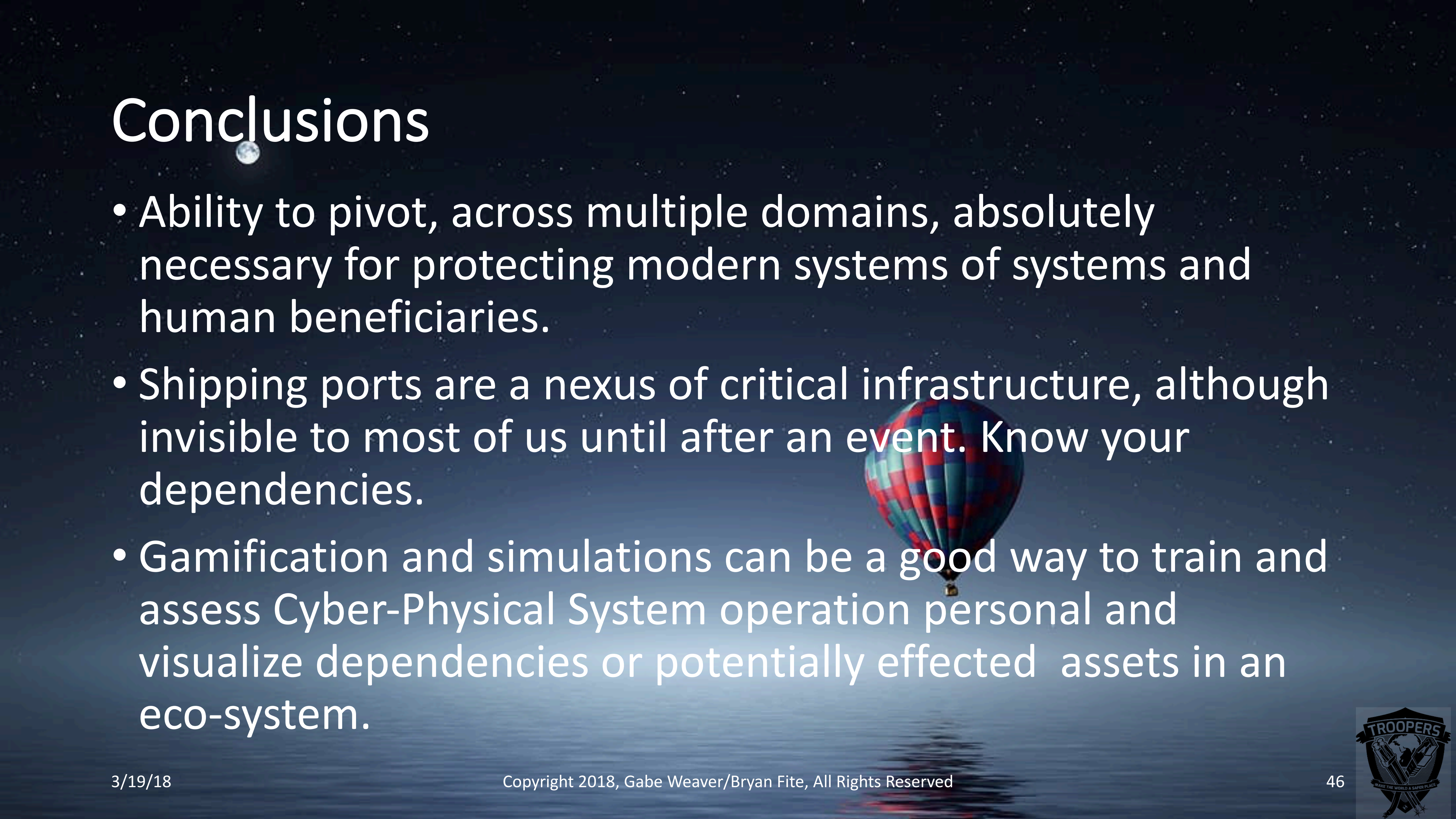


```
IF signal.power == OUT:
     signal.service_time *= 2;
```



Power

Transportation



Conclusions

- Ability to pivot, across multiple domains, absolutely necessary for protecting modern systems of systems and human beneficiaries.
- Shipping ports are a nexus of critical infrastructure, although invisible to most of us until after an event. Know your dependencies.
- Gamification and simulations can be a good way to train and assess Cyber-Physical System operation personal and visualize dependencies or potentially effected assets in an eco-system.