

Lavanya Marla

Glen Salo

Randy Sandone

Gabriel Weaver

Assessment and Measurement of Port Disruptions

Communities depend on the Maritime Transportation System (MTS).

- **Globally:** The MTS accounts for **more than 80% of global merchandise trade** in volume and 67% of its value in 2017.
- **Nationally:** The MTS accounted for **more than \$4.6 trillion of economic activity (1/4 of the US GDP)** in 2014.
- **Regionally:** Consider Port Everglades and Miami's tourism industry



100% Jet Fuel for Miami International Airport



100% Gasoline for S. FL

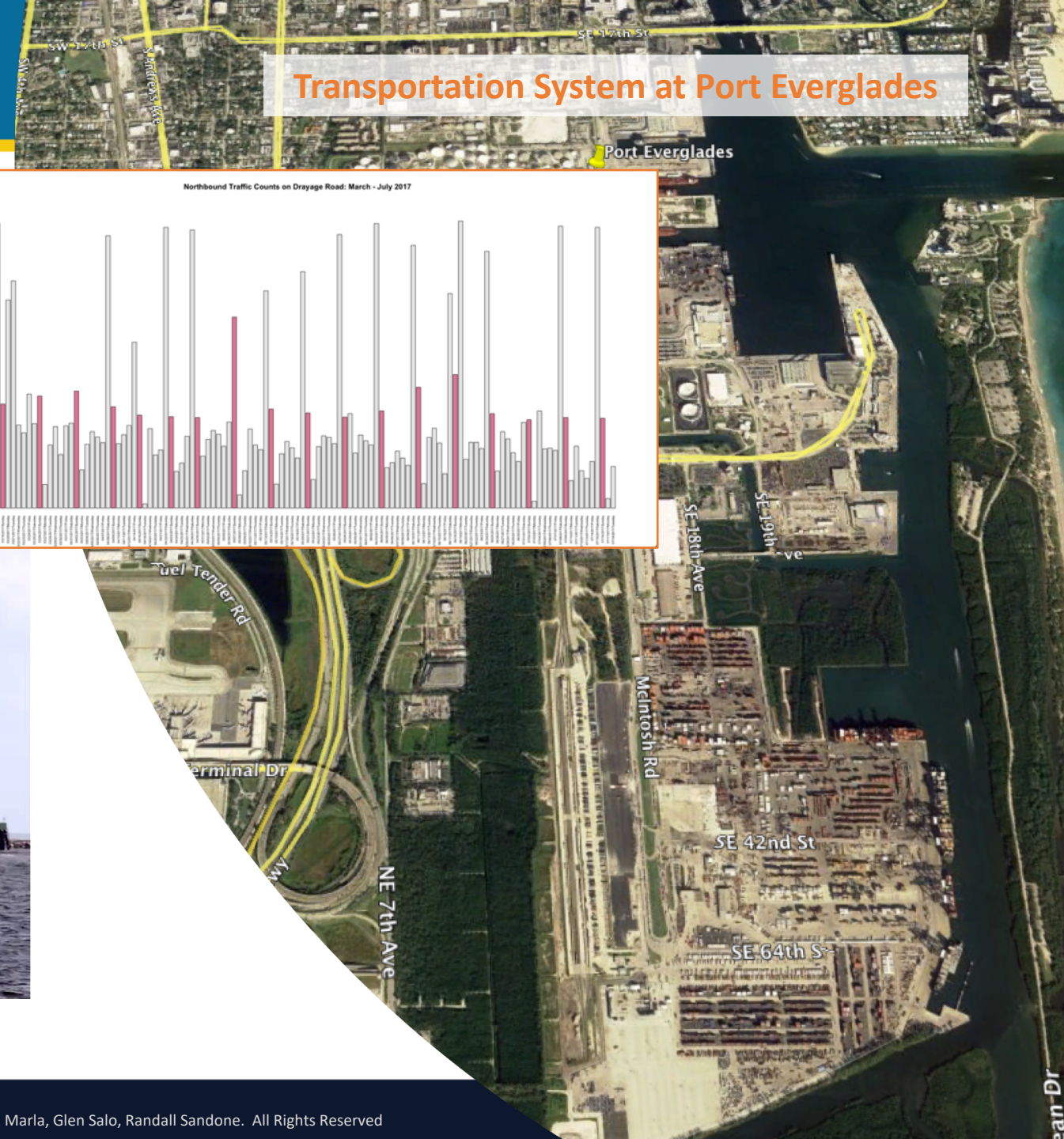


Food & Beverages

Transportation System at Port Everglades

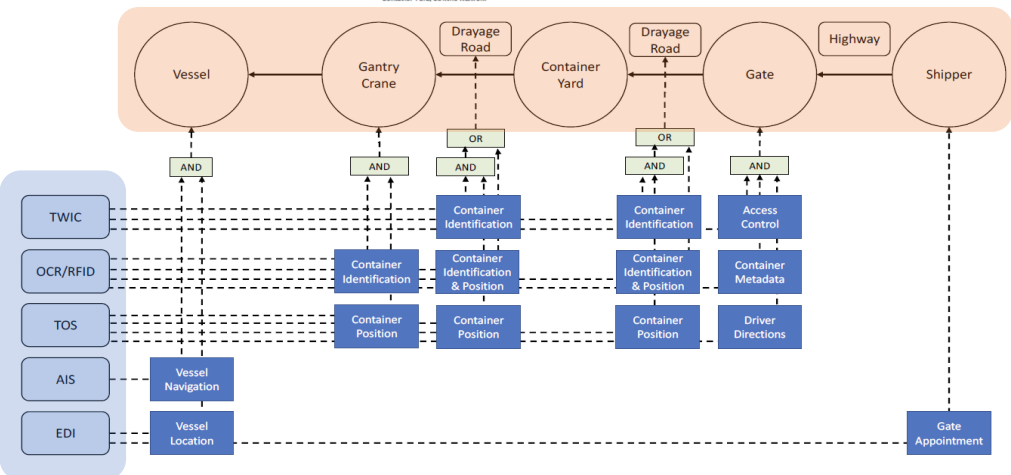
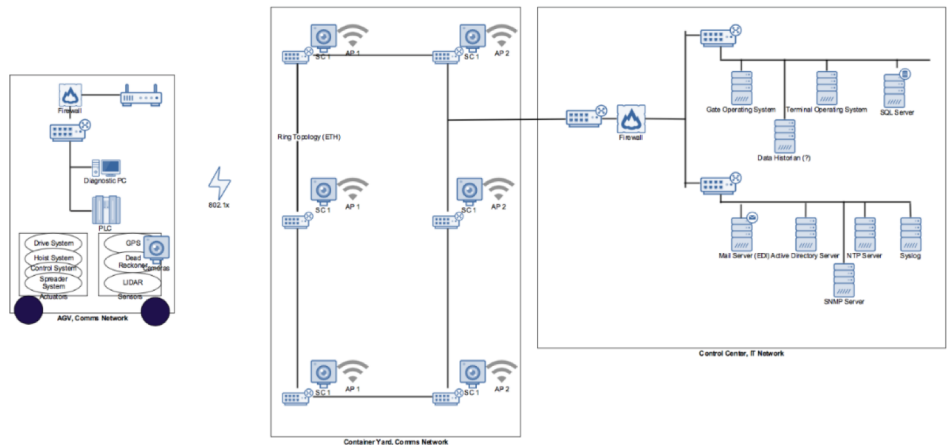
Shipping ports increasingly depend upon and are a nexus of critical infrastructure systems.

Intermodal Transportation System



Shipping ports increasingly depend upon efficiencies introduced by cyber systems.

Communications/IT System



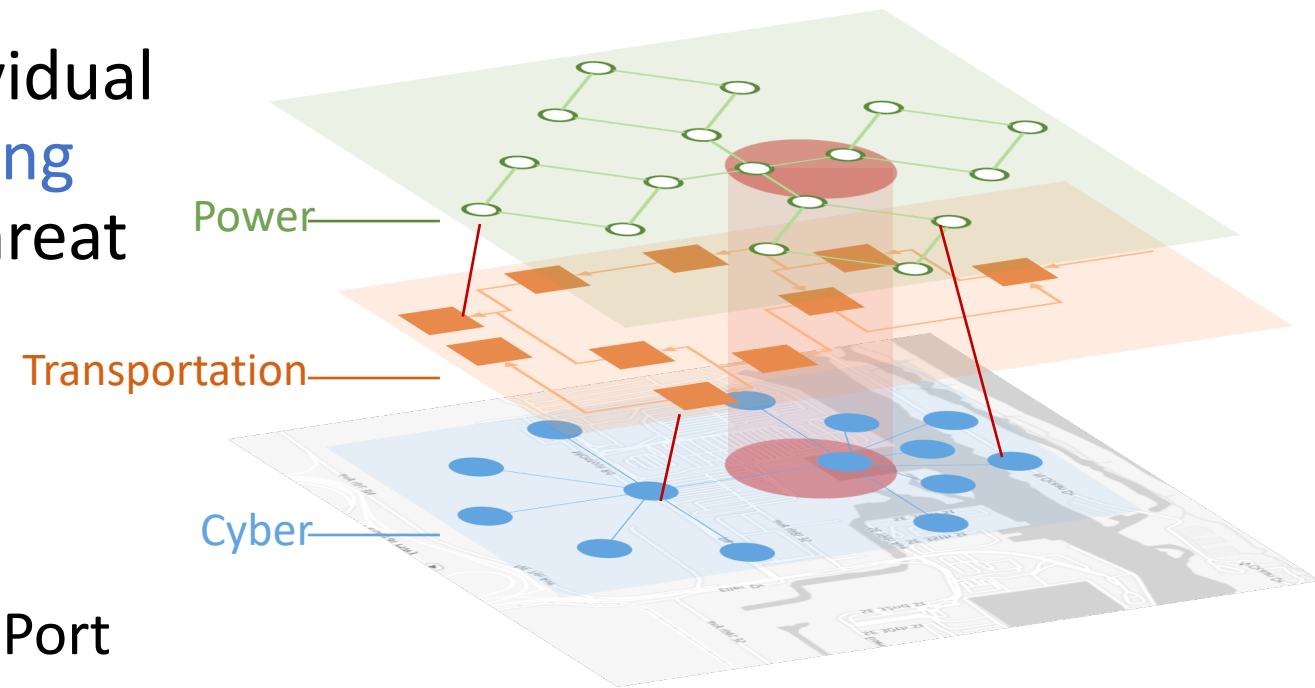
Communications/IT Systems at Crowley



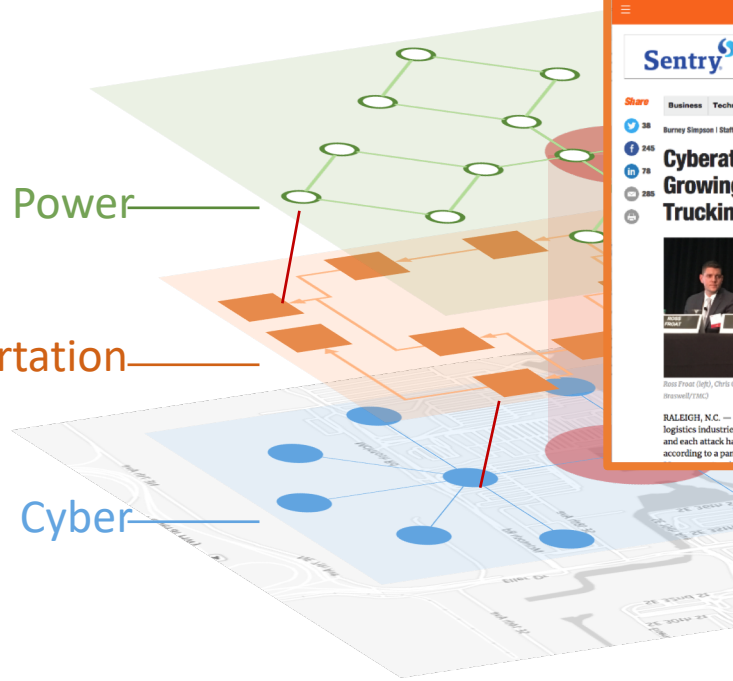
ID	Component
1	Gate Operating System (GOS)
2	Communications Network
3	Terminal Operating System (TOS)
4	Electronic Data Interchange (EDI)
5	Automatic Identification System (AIS)

Stakeholders need approaches to risk assessment relative to cross-infrastructure dependencies.

- Be **conducted continually** by individual ports for their **specific and changing** operational, technological, and threat **environments**.
 - Intelligent adversaries evolve
 - Environments evolve
- Provide results **rapidly**
 - Current, DHS-funded prototype for Port Everglades (PEV) delivers results in minutes



Stakeholders need approaches to evaluate functional and economic impact of disruptions relative to cross-infrastructure dependencies.



Sentry Protect your fleet. And your future.

Business Technology Equipment Autonomous

Share 38 245 78 285

Cyberattacks Called a Growing Threat to Trucking Industry

By Burley Simpson | Staff Reporter June 7, 2018 1:30 PM, EDT

Trending

- 1 Teamsters, YRC Strike Tentative Deal on Labor Contract
- 2 CVSA's Collis Money: Trouble

DARK TIMES

Photos: A massive petrochemical fire in Texas will burn for days

By Jimmy Stone March 16, 2018

Official website of the Department of Homeland Security

CISA
CYBER-INFRASTRUCTURE

HOME ABOUT US ALERTS AND TIPS RESOURCES C*VP

Potential Hurricane Harvey Phishing Scams

Original release date: August 28, 2017 | Last revised: September 20, 2017

Print Tweet Send Share

US-CERT warns users to remain vigilant for malicious cyber activity seeking to capitalize on interest in Hurricane Harvey. Users are advised to exercise caution in handling any email with subject line, attachments, or hyperlinks related to Hurricane Harvey, even if it appears to originate from a trusted source. Fraudulent emails will often contain links or

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

State Tech TOPICS STATES TIPS & TACTICS VOICES FEATURES VIDEO IT BLOGS MORE + LOG IN

HOME SECURITY

Port of San Diego Continues to Recover from Ransomware Attack

Recent attack highlights the importance of data backups in the face of ransomware threats.

by Phil Goldstein

Phil Goldstein is the web editor for FeedTech and State Tech. Besides keeping up with the latest in technology trends, he is also an avid lover of the New York Yankees, poetry, photography, traveling and escaping humidity.

The Port of San Diego, which disclosed last month that it had suffered from a ransomware attack on Sept. 25, continues to recover from the attack.

The port has continued to operate, but some computer and IT systems remained offline as of last week, according to The San Diego Union-Tribune. The port is working with state, local, regional, state and federal experts to restore its systems, the newspaper reports, and the FBI and Department of Homeland Security are part of the investigation.

Latest Articles

- New Sensors Will Monitor Michigan's Mackinac Bridge
- Innovate Ohio Looks To Modernize Public Services
- Review: The Canon Lx-M1500 Can Do It All When It Comes To Presentations
- Why Local Agencies Should Develop Cybersecurity Plans

BBC NEWS

Police warning after drug traffickers' cyber-attack

By Tom Bateman Reporter, Today programme

16 October 2013

Share

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

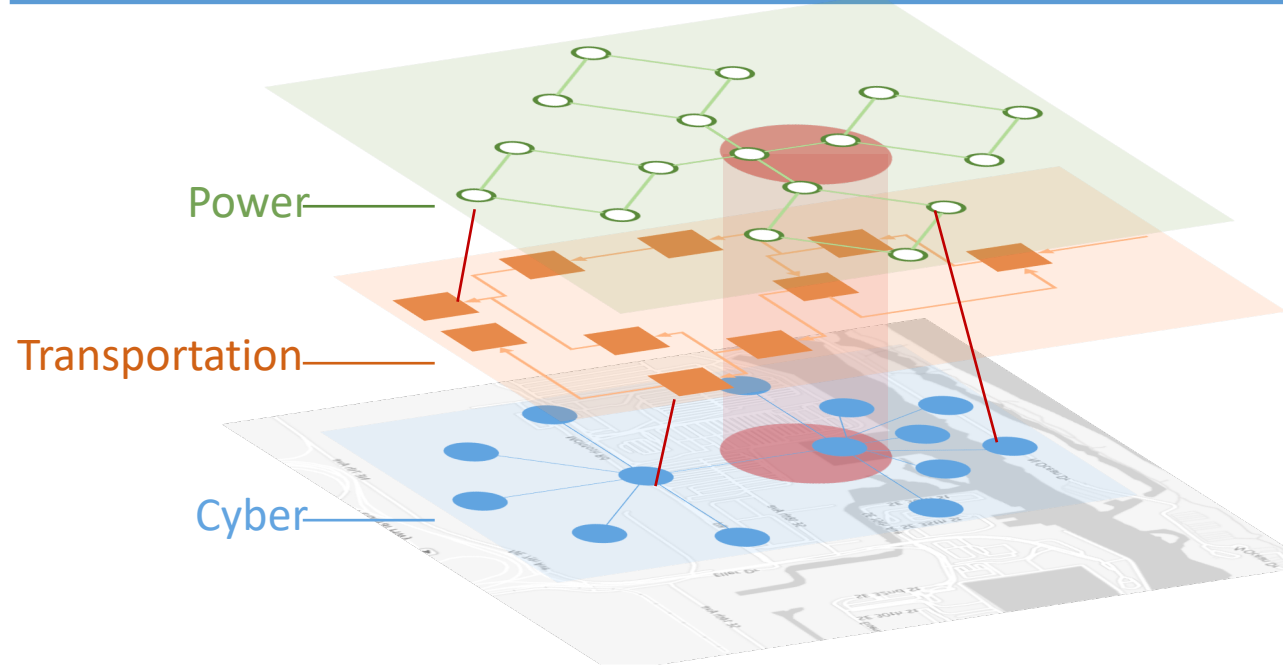
The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

His comments follow a cyber-attack on the Belgian port of Antwerp.

Intended Outcome

- Illuminate cross-organizational, functional dependencies on infrastructure.
- Rapidly identify impacts from possible coordinated disruptions to stakeholder missions
- Prioritize investments to plan and respond to all-hazards that may affect mission
 - Prevention
 - Mitigation

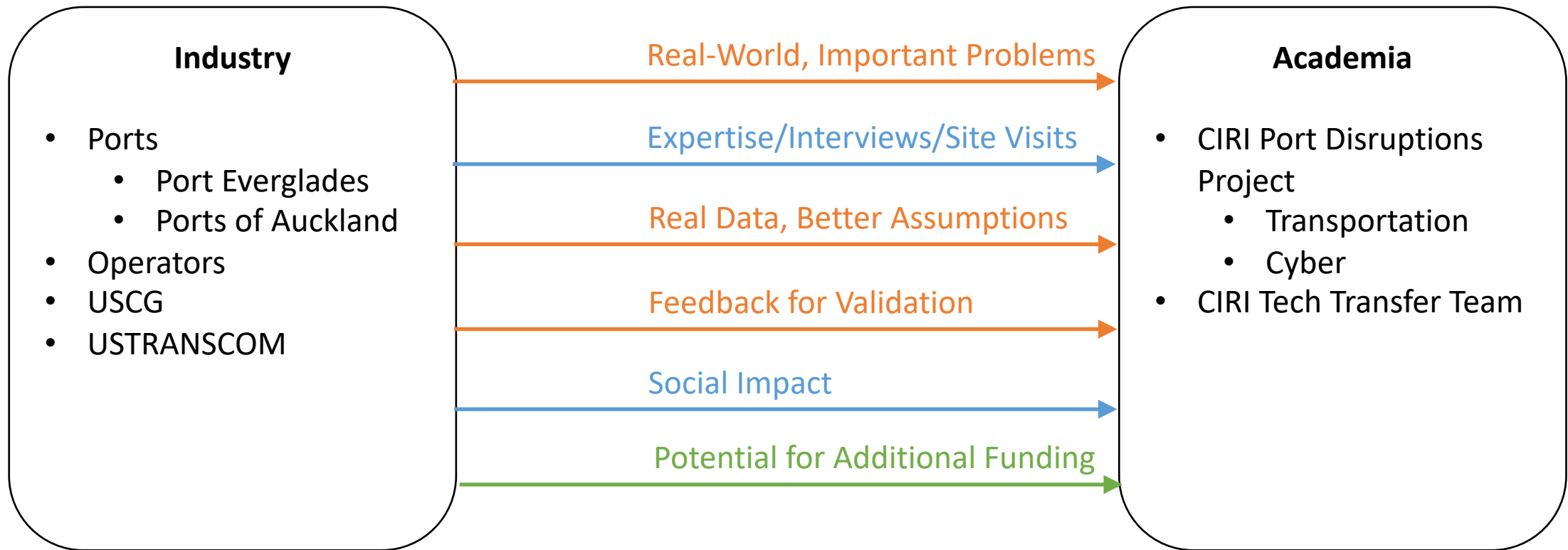
Location



Time

Left of Boom	Boom	Right of Boom
<ul style="list-style-type: none"> • Training Exercises • Area Maritime Security Plans • FEMA Port Security Grants 	<ul style="list-style-type: none"> • Determine the effects of mitigation strategies • Compute optimal mitigation actions 	<ul style="list-style-type: none"> • Evaluate response and recovery strategies • Evaluate strategies to improve port operations.

Benefits for Academia: Intellectual, Social, and Financial



Benefits for Industry: Intellectual, Social, and Financial



Thank You!

- Department of Homeland Security
- US Coast Guard
 - USCG Sector Miami
 - USCG Research & Development Center
- Ports of Auckland
- Port Everglades
 - Broward County Sheriff's Office
 - Customs and Border Protection
 - Crowley
 - Florida East Coast Railway
- USTRANSCOM



U.S. Customs and
Border Protection

