PortSec: A Port Security Risk Analysis and Resource Allocation System

Michael D. Orosz, Ph.D.
Computer Scientist
Lead, Decision Systems Group
mdorosz@isi.edu
310-448-8266

Information Sciences Institute
Viterbi School of Engineering
University of Southern California
Marina del Rey, CA

Isaac Maya, Ph.D. PE
Director of Research
CREATE
imaya@usc.edu
213-740-3865

University of Southern California
Los Angeles, CA

9 November 2011

Outline

- Problem addressed
- What is PortSec?
- Current status of project
  - Incident response
- Next steps
  - Complete Tactical
  - Cyber/Physical Infrastructure
  - Strategic Analysis

Research Support

This research is supported by the United States Department of Homeland Security (DHS) through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-00001. However, any opinions, findings, and conclusions or recommendations in this presentation are those of the authors and do not necessarily reflect views of the US DHS.

The Problem – Three Competing Needs

- Protection of the ports: security
  - Provide jobs (locally and nationally)
  - Support import/export business
  - Critical component of the Nation's supply-chain.
  - **They are a major target of terrorism**
- Economic viability: goods *must* flow
  - Need to minimize interruptions to business or increased cost of doing business
  - **Excessively costly/disruptive protection causes economic harm to US, satisfies terrorist aims**
- Environmental costs: green ports
  - **Throughput delays due to security counter-measures impact the environment**

Improve port security, minimize cost to business and environment

The Challenges

- System of systems: Ports and similar operations are composed of many different components (e.g., terminals, bridges, inspection points, etc.,), agencies, and interactions between these "systems"

- Dynamic operations: These "system of systems" are dynamic - constantly changing both day-to-day and long-term.

Complex dynamic infrastructure -> difficult to model and analyze

Example Challenge: Over 13 different resources involved in POLA/LB security

- Los Angeles Port Police
- Port of Long Beach Harbor Patrol
- Los Angeles Police Department Harbor Division
- Long Beach Police Department
- California Highway Patrol
- U.S. Coast Guard
- U. S. Customs and Border Protection
- Los Angeles County Fire Department
- City of Long Beach Fire Department
- City of Los Angeles Fire Department
- U. S. Immigration and Customs Enforcement
- Los Angeles County Sheriff's Department
- Federal Bureau of Investigation
- Others…

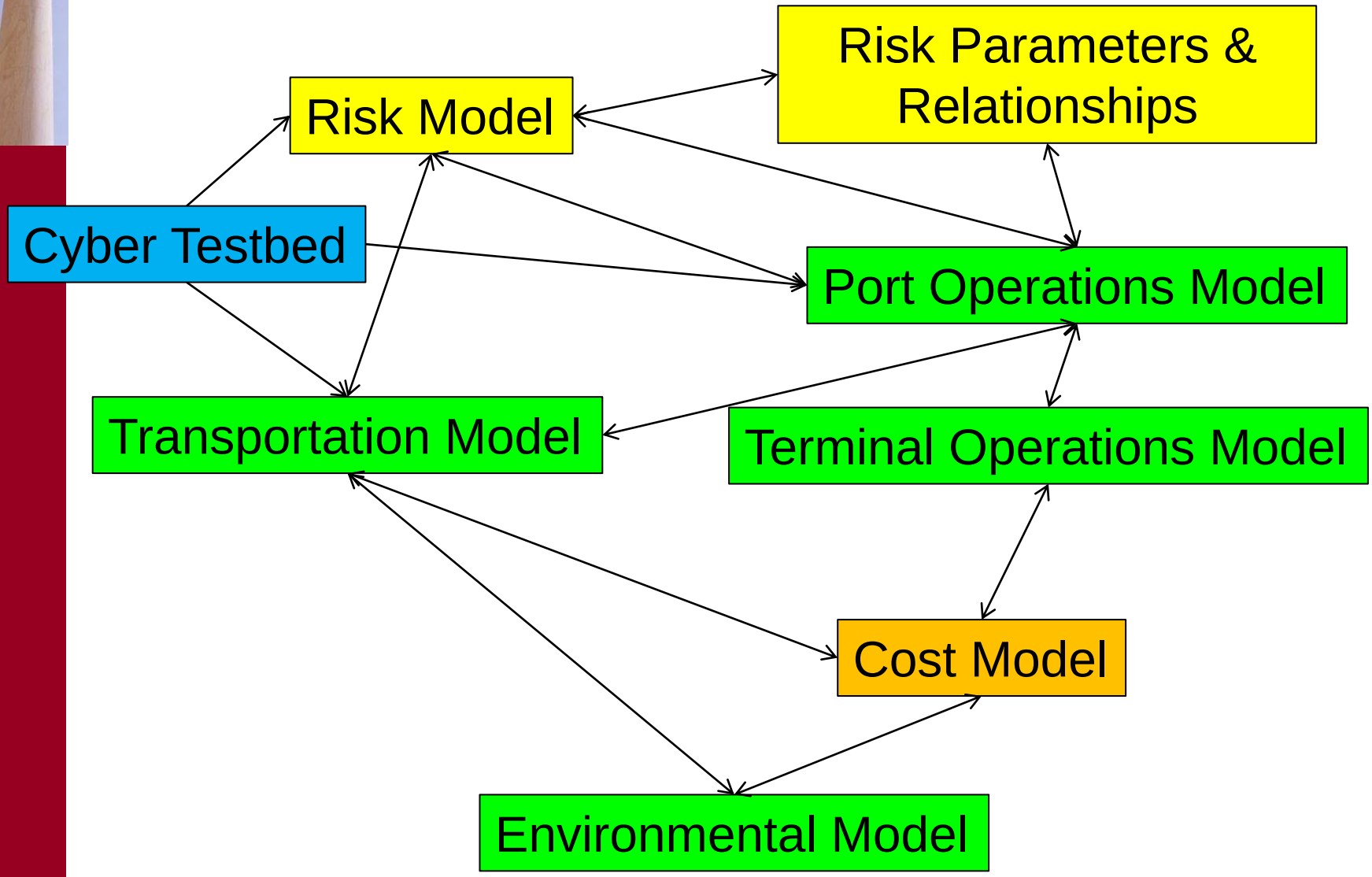
Goal: Can collaboration and resource allocation be improved?

PortSec

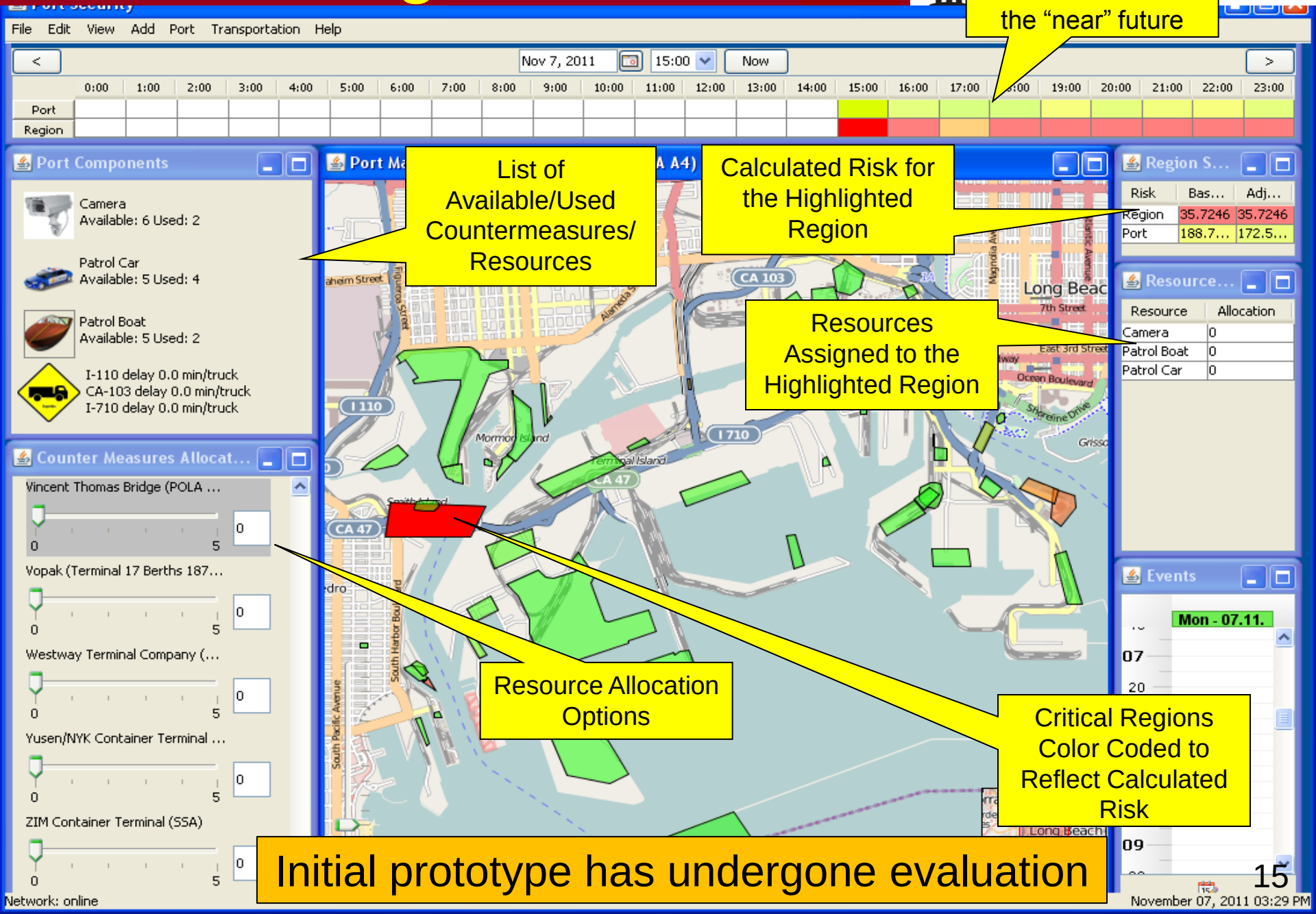
- A resource allocation system used to reduce risk primarily from terrorist-based attacks (**for now**)
  - Maintain port operations (business resiliency)
  - Minimize impact to environment
  - Addresses ***trade-offs*** between maintaining operations vs. minimizing risks from attack (includes minimizing consequences)
- **Tactical**:
  - Day-to-day adjustments of resources to reduce assessed risk of attack
  - Real-time incident response (**current focus**)
- **Strategic**: "what-if" analyzes to determine impact on port security due to future events (**longer-term**):
  - New counter-measures
  - Port improvements/modifications

Trade-off: Minimize threats vs. maintain port Ops vs. environment

Fundamentals: System of Systems



Tactical Usage: Port Security Officer



Initial prototype has undergone evaluation

Status

- Prototype 1.0: Supports tactical operation
  - Reviewed by POLA/LB – strong support
  - Regions of interest are based on MAST study
  - Risk assessment parameters & attack modes are based on MAST study
  - Currently updating risk model to reflect results from expert elicitations (which are on-going)
  - External systems (e.g., Marine Exchange) are simulated

Prototype 1.0 exhibits the look, feel, and performance of the actual system

Prototype 1.0: Working prototype undergoing evaluations

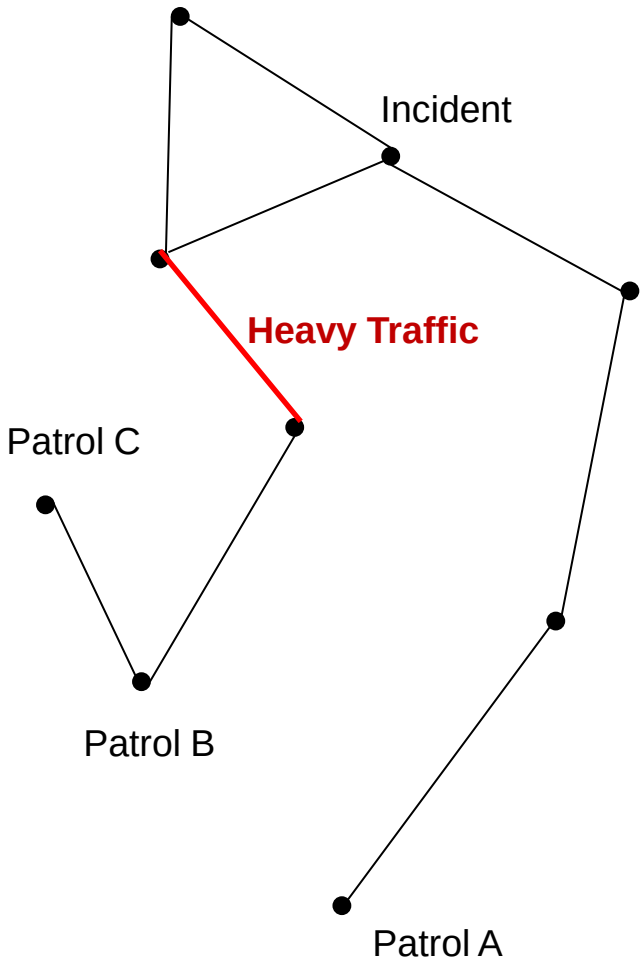
Next Steps

- Implement demonstration incident response (**current focus – Dec 2011/Feb 2012**)
  - Teaming with SAIC – link PortSec to UICDS
  - Establish connections with external data sources (i.e. no longer simulated)
    - Marine Exchange
    - CalTrans
  - Immerse into POLA Police operations
  - Update risk assessment model
- Complete tactical support development (**May/June 2012**):
  - Implement calendar-based event support
  - Establish remaining connections to external data sources (e.g., blue force tracking)
  - **Establish connections to intelligence sources (e.g., SARs)**
  - Complete modifications to risk assessment model

Goal: Mid 2012 - Tactical version of PortSec installed at POLB/LA

Incident Response – Resource Allocation

- Don't want to over-allocate resources
- Resource allocation based on:
  - Distance to incident scene
  - Priorities
  - Capabilities of the resource
- Distance calculation – based on:
  - Time of day
  - Current congestion
- Backfill
  - Cover "space" left vacant



Cyber-Infrastructure

- Major Challenges faced today:
  - Understanding impact a cyber attack can have on the Nation's physical infrastructure
  - Demonstrating to stakeholders the impact a cyber attack can have on their operations
    - Includes both direct and indirect economic costs
    - Public health
    - Symbolic
- Next Steps:
  - Link the DHS-funded DETER cyber testbed to PortSec. DETER allows:
    - Simulation of IT infrastructure
    - Simulation of cyber attacks (single or multiple)
  - Link to a macroeconomic model – Adam Rose

Linking cyber attack testbed to physical infrastructure models

Cyber-Infrastructure

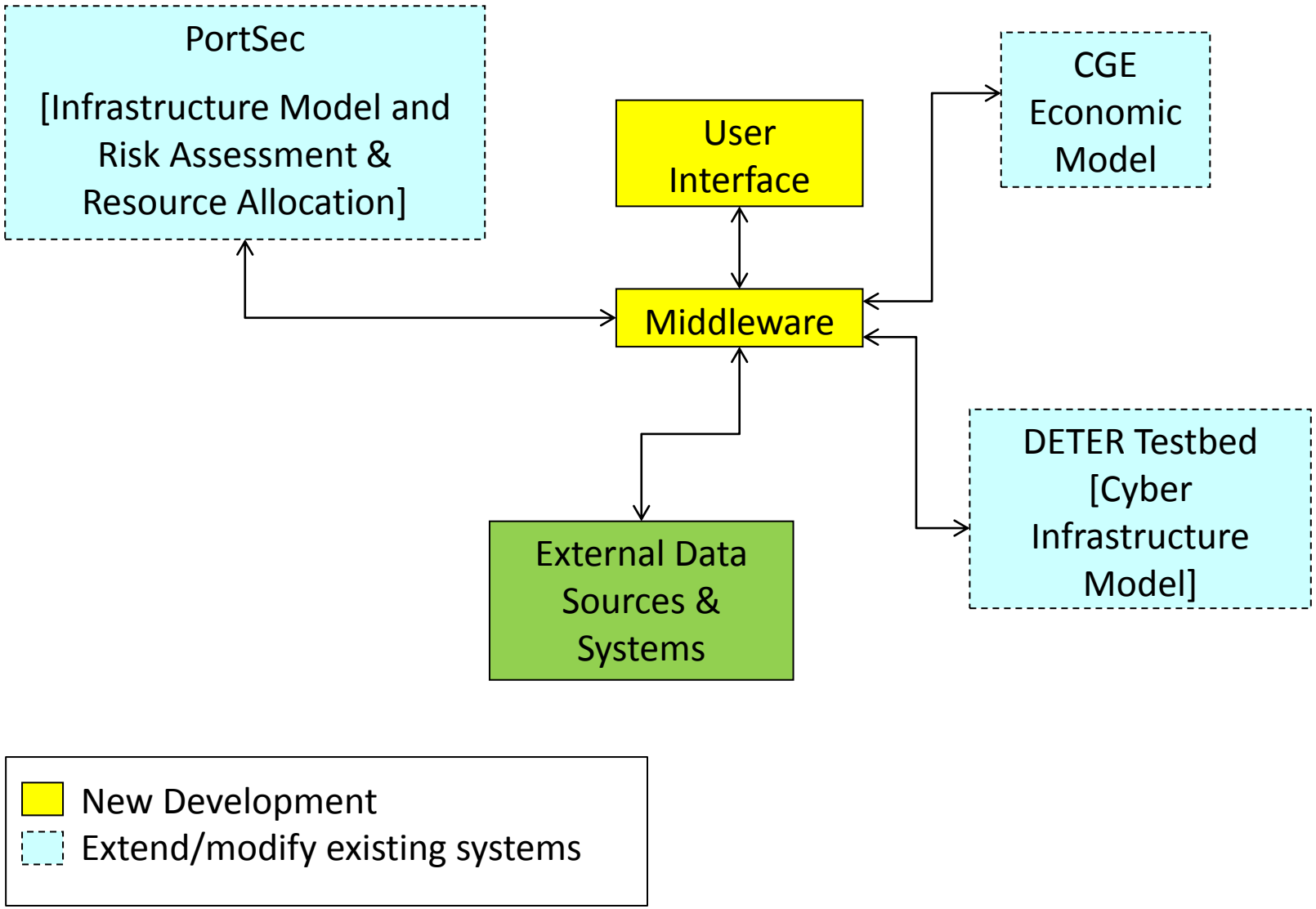


Photo Credit: POLA

Thank You