

Cyber: A Critical New Domain for GIS

Brian Biesecker

David Attaway

Wendy Creighton

What are the Fundamental Problems that GIS can help you solve?

- What are the impacts to your mission, operations, business activities, or critical systems from a Cyber Attack, IT outage or impairment?
- How do you prioritize the work of your IT Team or Cyber Security Team in the context of your most important missions, operations, business activities or critical systems?
- How do you provide shared situational awareness across your organization?

Cyberspace Re-Considered

It's Mappable

ArcSchematic

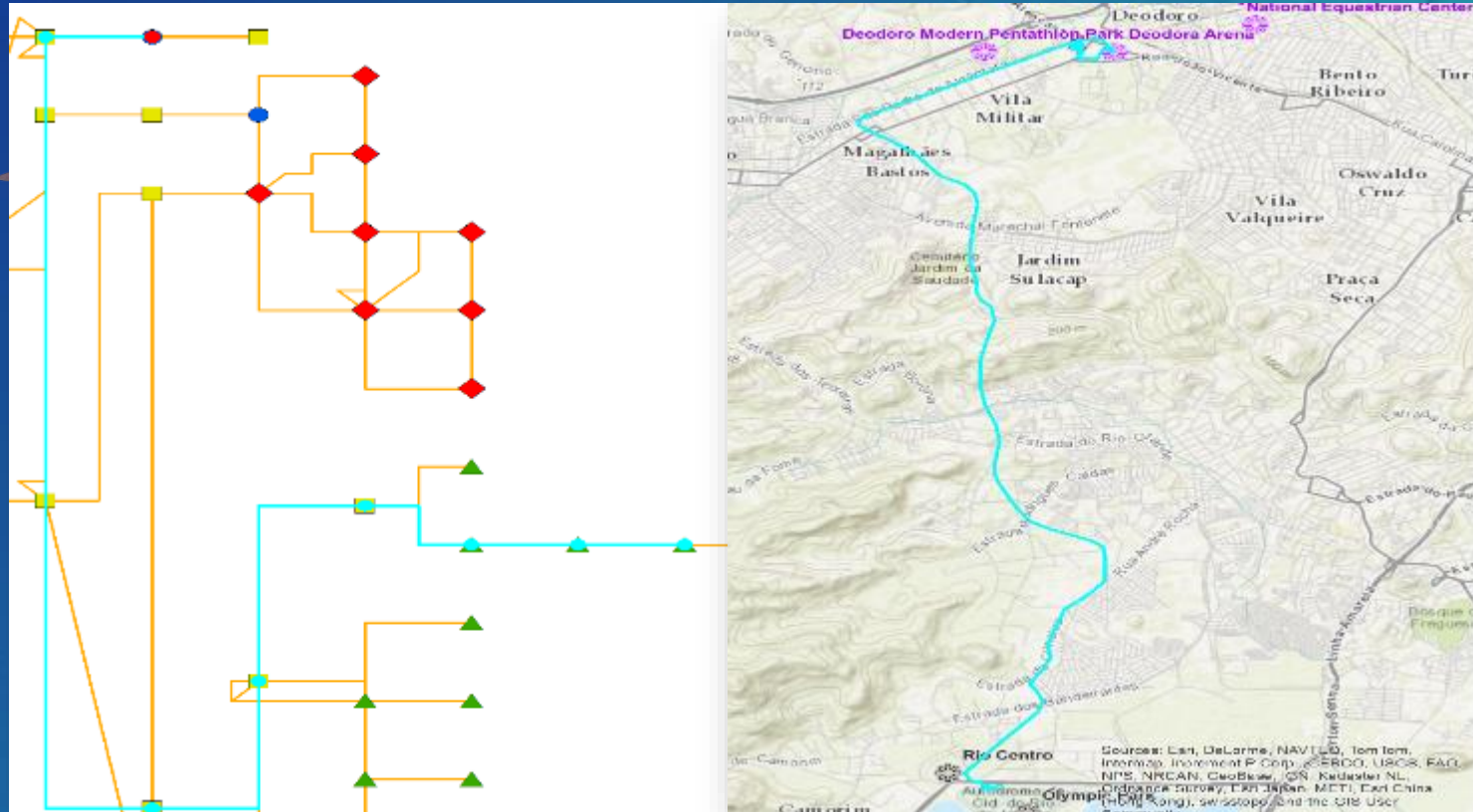
Social / Persona Layer

Device Layer

Logical Network Layer

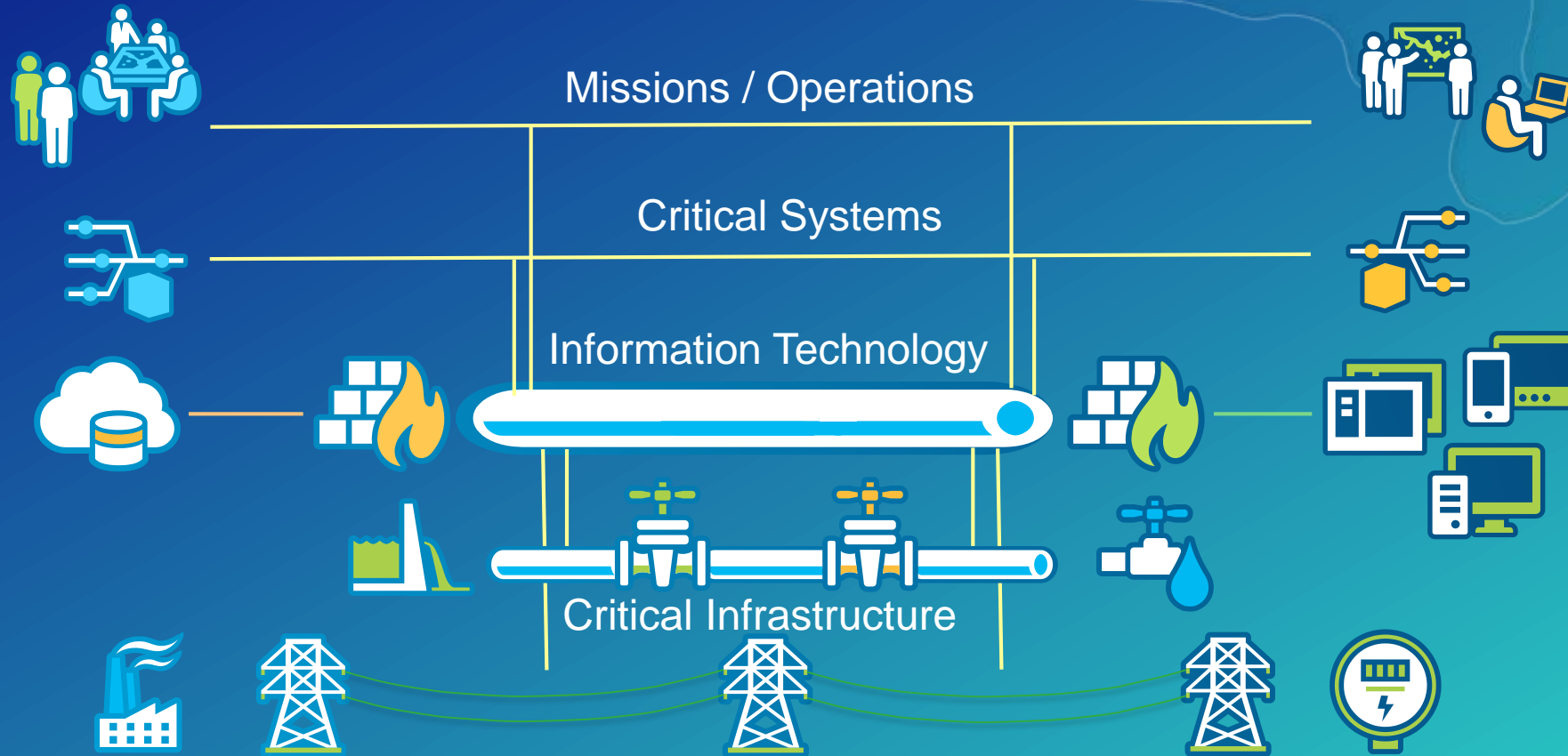
Physical Network Layer

Geographic Layer



- Each device in cyberspace is owned by someone (no 'global commons')
- Electro-mechanical devices exist in space-time and interact with physical events
- Geography is required to integrate and align cyberspace with other data

Applies to many domains



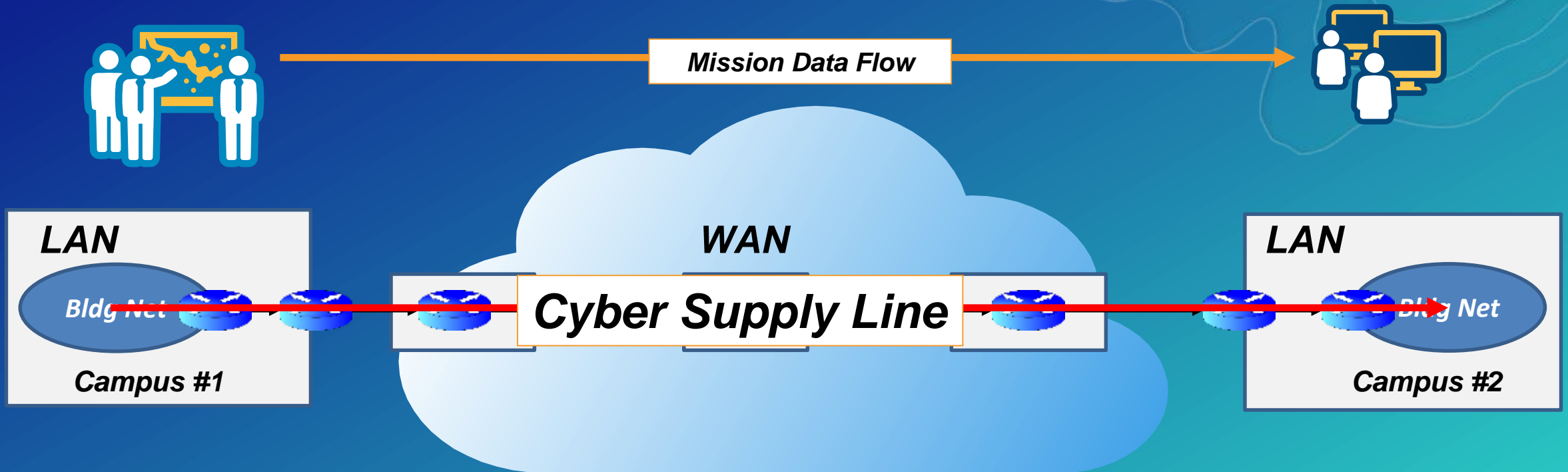
Solution Strategy

Integrating to improve awareness



The Cyber Supply Line

A vector of devices



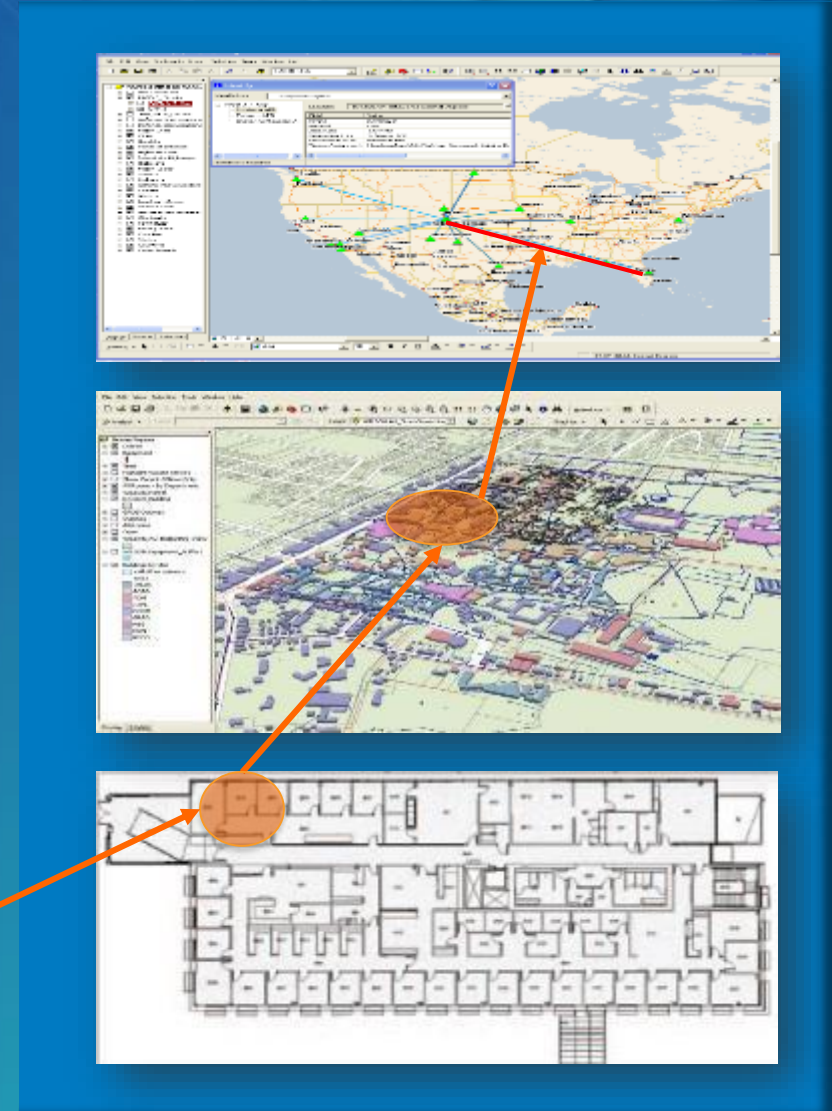
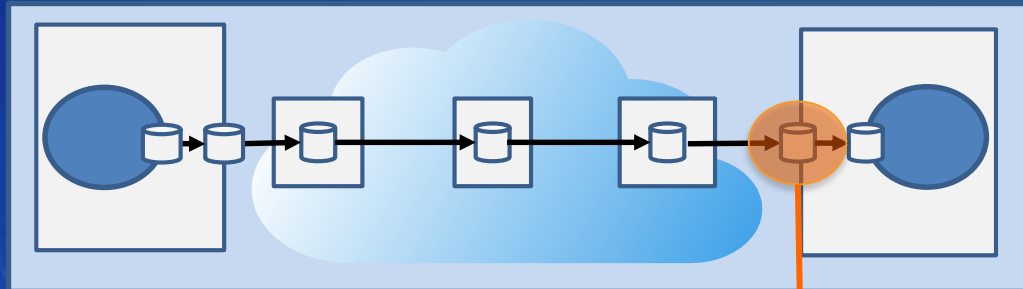
- Cyber Supply Line (CSL) is a *consistent* path through the infrastructure
- CSL focuses resources on only the devices that are critical
- Managing data flows is similar to traffic routing; an Esri core competency

Effect Propagation

Multi-level Model of Data Flow

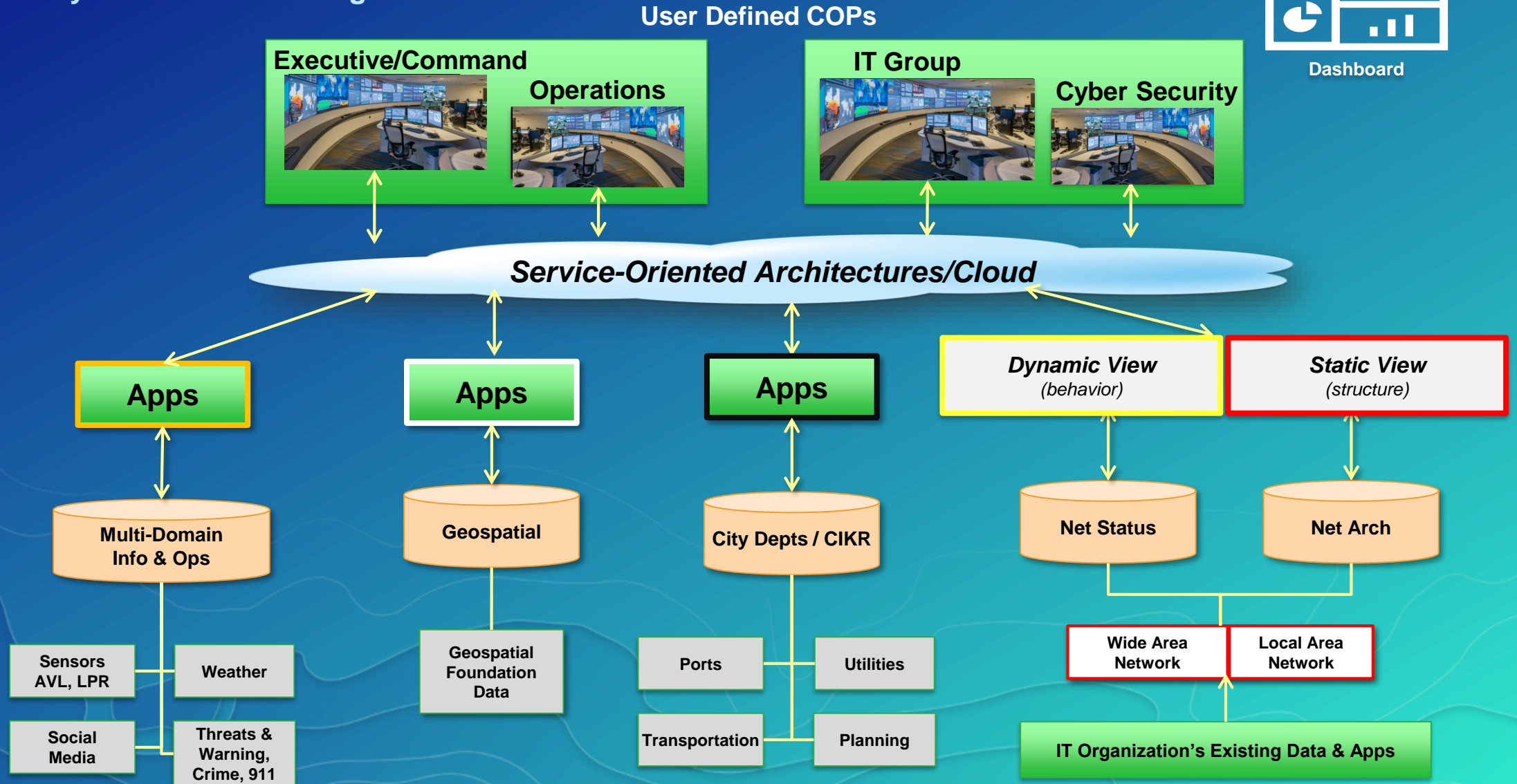
Cyber Supply Line

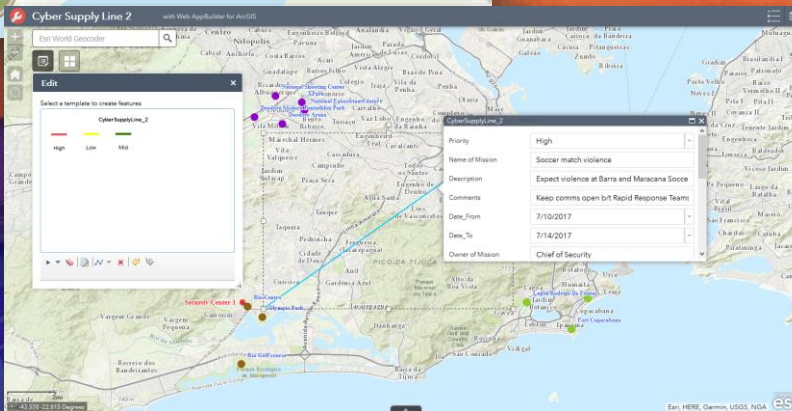
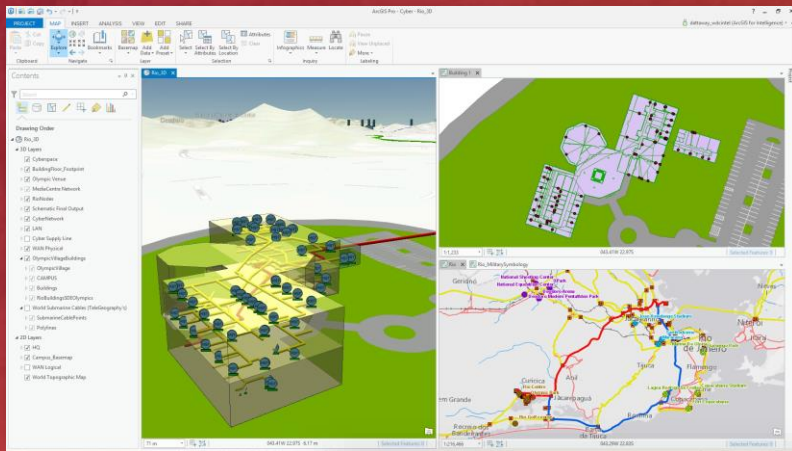
Maintain Data Flow → Mission Assurance



Solution Strategy

Integrate Cyber into the existing ArcGIS Platform





Rio 2016 Olympic Games

David Attaway

ArcGIS Integration with Cyber Security Tools

Executives



Executive Dashboards -
Status Reports, Trends,
Brand Sentiment, Financials

Cyber Security

Cyber Tools & Data -
IDS/IPS, HBSS, Virus Scanning,
Patch Monitoring



Operations



Ops Data -
Mission Activity, Status Reports,
Real-time monitoring



Portal



IT Operations

IT Tools & Databases -
IT Inventory, Device Locations,
Health and Status Monitoring



Human Resources



HR Database -
Personnel, Orgs,
Locations, Travel

Facilities

Facilities Data -
CAD & GIS of
Buildings and Campuses,
Electric, Water, HVAC, Facilities
Monitoring, Physical Security



Linking your data to create the necessary relationships

Human Resources Database		
Person	Org	Location
Bill	Team 1	2Q001
John	Team	
Sue	Team	
Rick	Team	
June	Team	
Eva	Team	
Dan	Team	

IT Inventory Database		
Person	Device	Ident
Bill	PC1	00:00
John	PC	
Sue	PC	
Rick	PC	
June	PC	
Eva	PC	
Dan	PC	

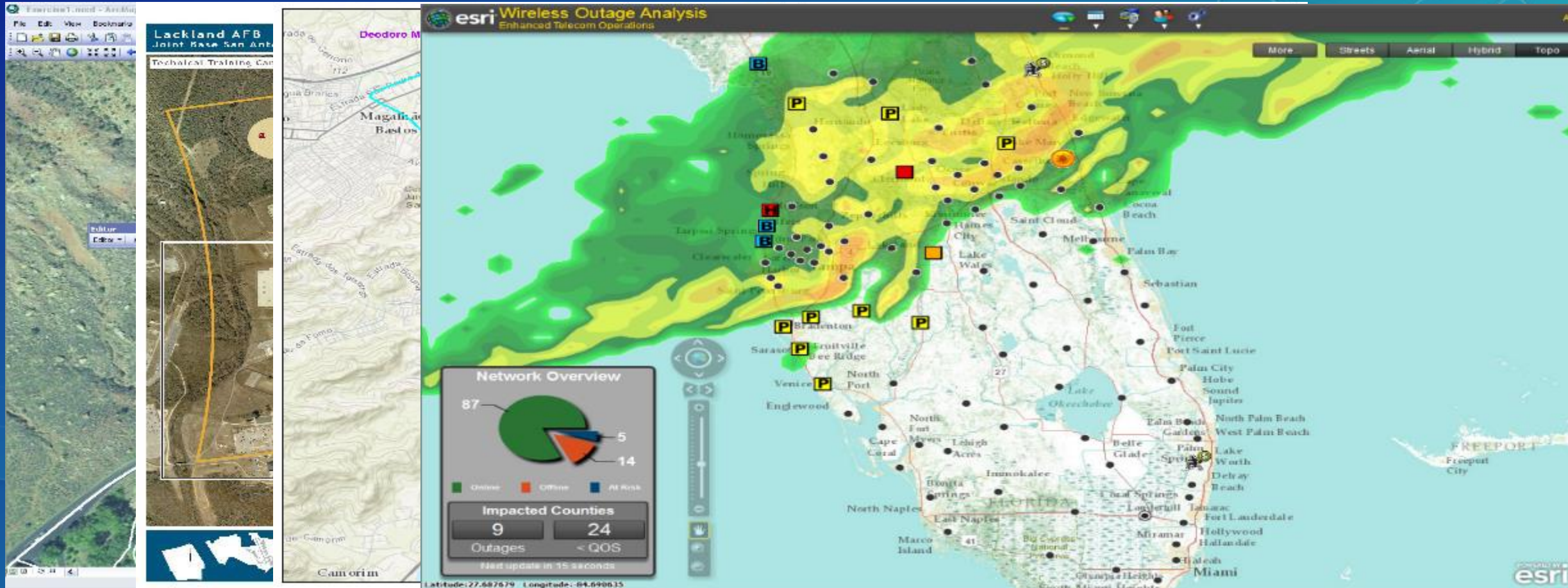
Mission	Orgs	Personnel
Rapid Response Team	Team 1	Bill
	Team 1	John
	Team 1	Sue

2Q001	xxx.xxx.32.250
2Q002	xxx.xxx.32.251
2Q003	xxx.xxx.32.252
1W003	xxx.xxx.32.240
1W004	xxx.xxx.32.241
1W005	xxx.xxx.32.242
1W006	xxx.xxx.32.243

Data Linkages

• Mission / Operational activities	to	Organizations / People
• Organizations	to	People
• People	to	Their location
• People	to	Devices they use
• Devices	to	Their location
• Devices	to	Their logical network connection
• Logical Network	to	Physical Network
• Logical / Physical Network	to	Network Devices
• Cyber Threats	to	Devices
• IT Health and Status	to	Devices
• Impacted Devices	to	Impacted Mission

Cyber Summary

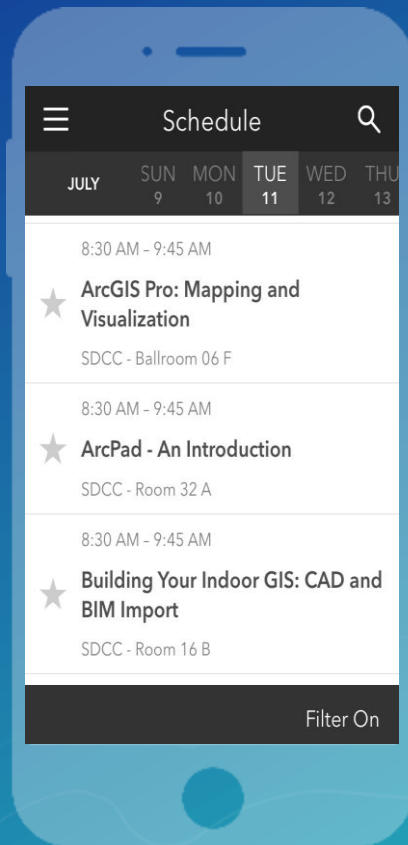


Please Take Our Survey on the Esri Events App!

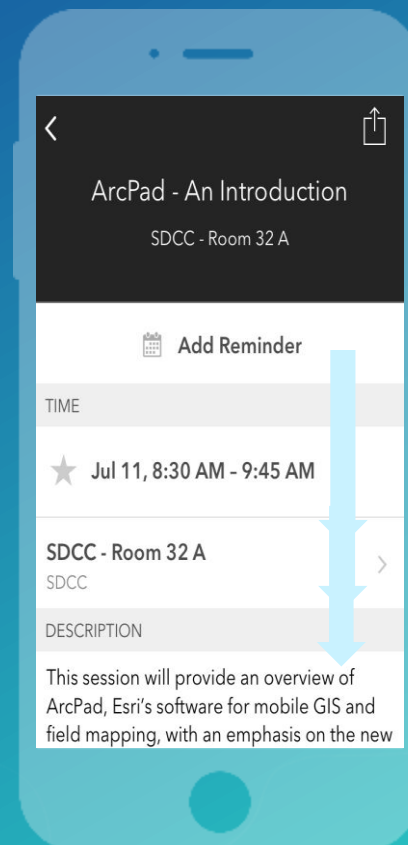
Download the Esri Events app and find your event



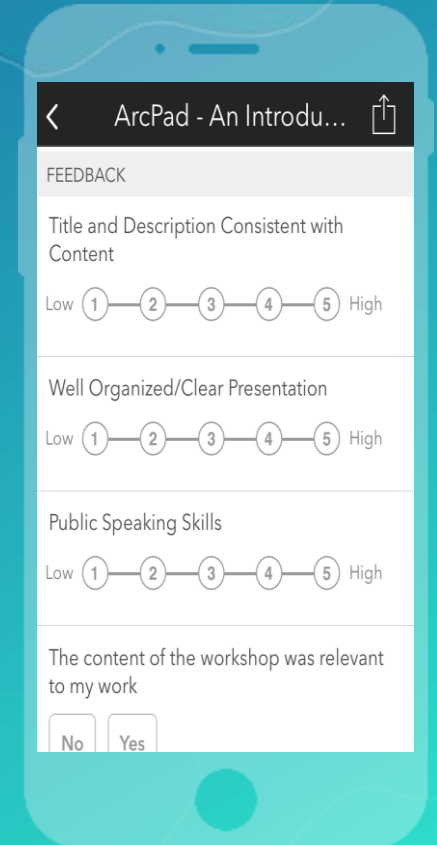
Select the session you attended



Scroll down to find the survey



Complete Answers and Select "Submit"





esri

THE
SCIENCE
OF
WHERE