Time and Space: Convergent Monitoring of the Cyber Supply – a Geospatial Approach

Presented by **Brian Biesecker**, Technical Director, Esri

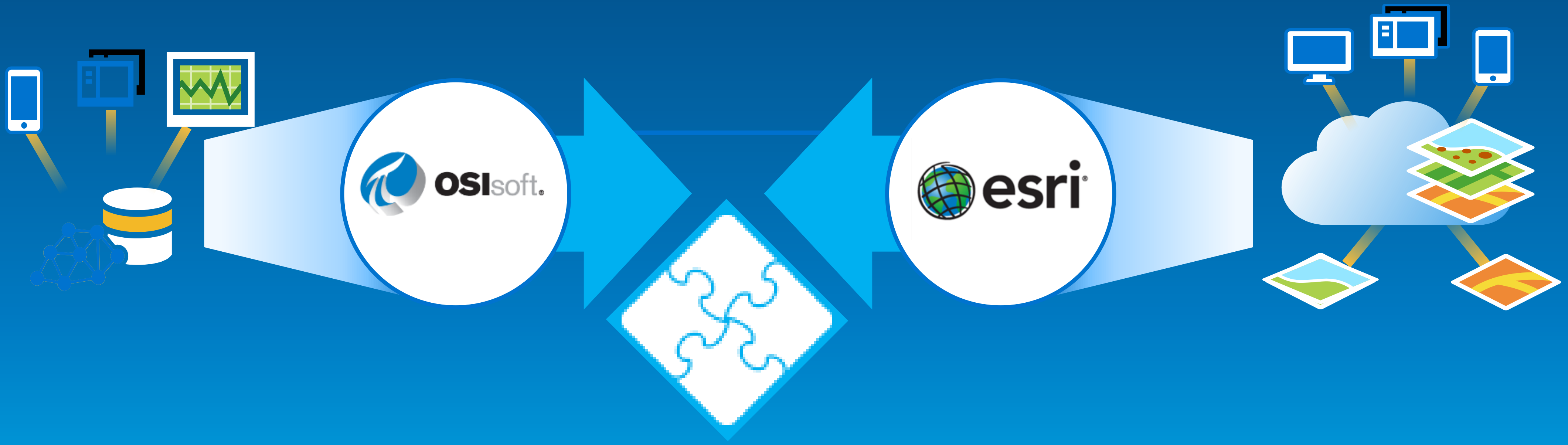
Cyber-GIS

GIS provides critical understanding

Brian Biesecker, Esri

Two Companies One Vision:

We believe data in the hands of smart people can create amazing insights, business improvements, and value



Time & Space

An Integrating Framework for Intelligence and National Security

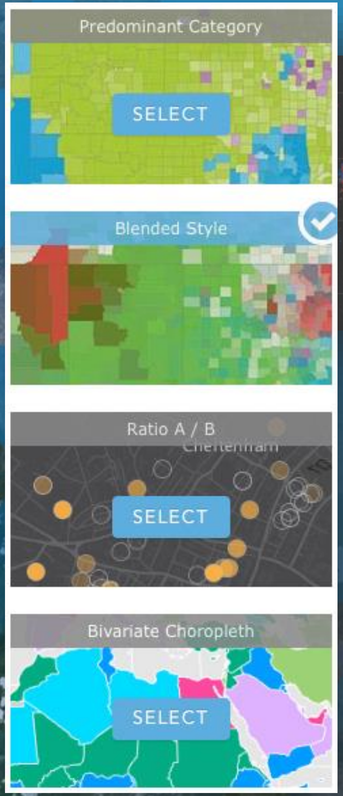
Lots of Sensors generate data…

These Sensors are increasingly connected…

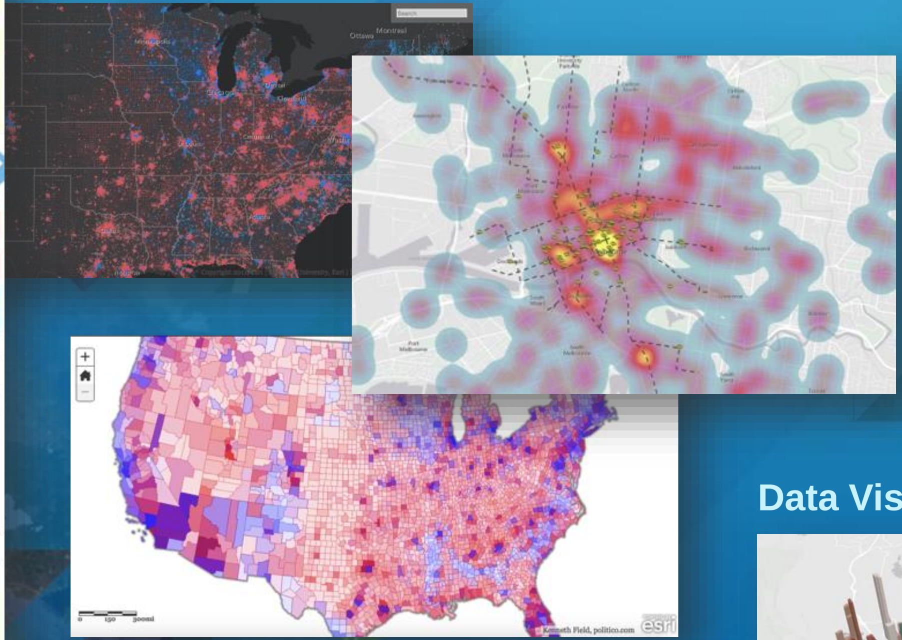
50 billion devices will be connected by 2020

At Esri, we look at Sensors geospatially

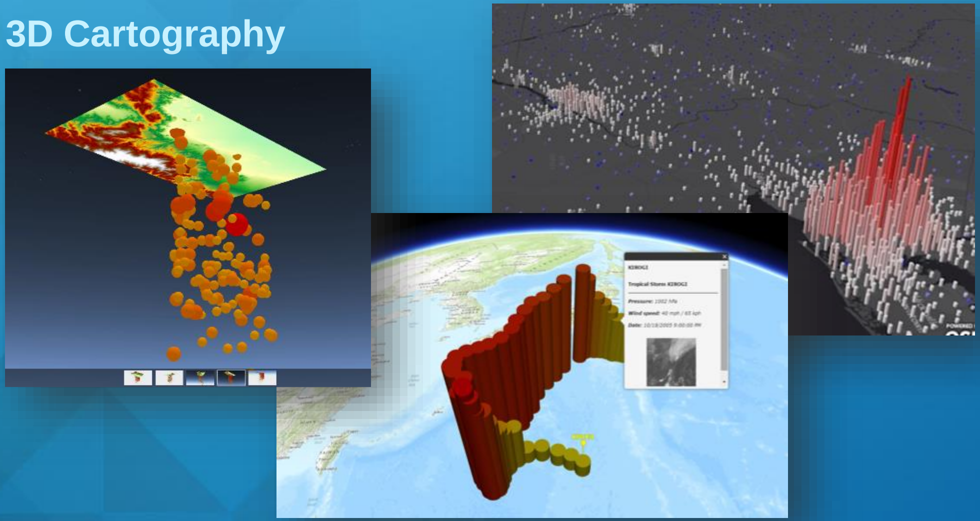
Visualize in Time & Space



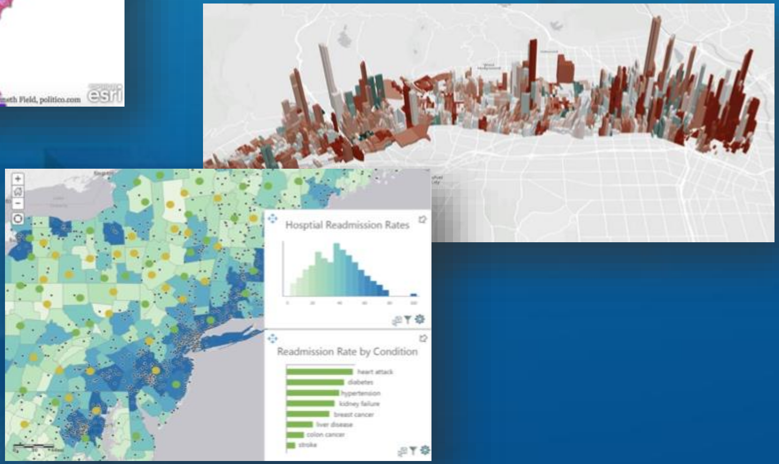
Smart Mapping



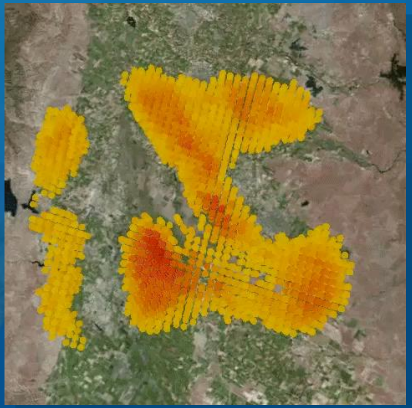
3D Cartography



Data Visualization

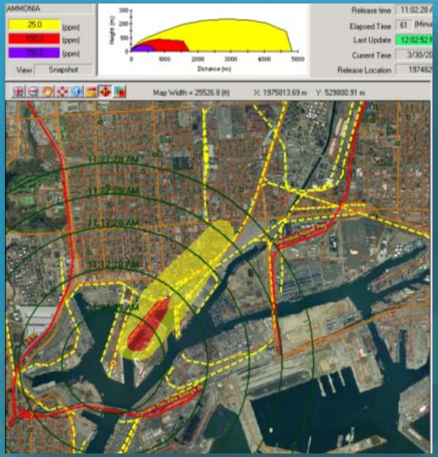


Data Exploration



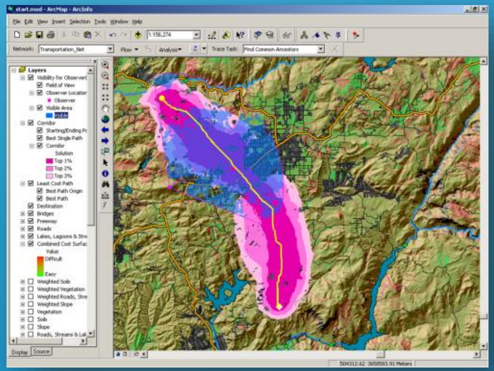
Analyze in Time & Space

Plume Modeling

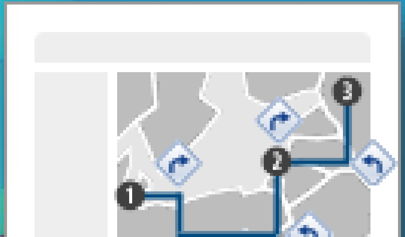


Location Allocation

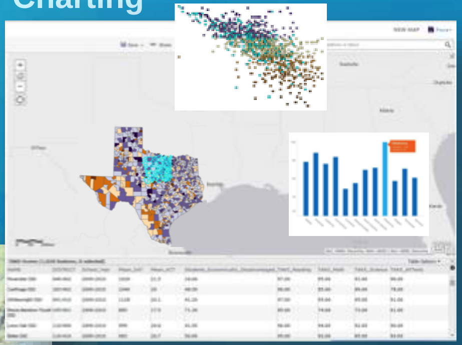
Mobility Analysis



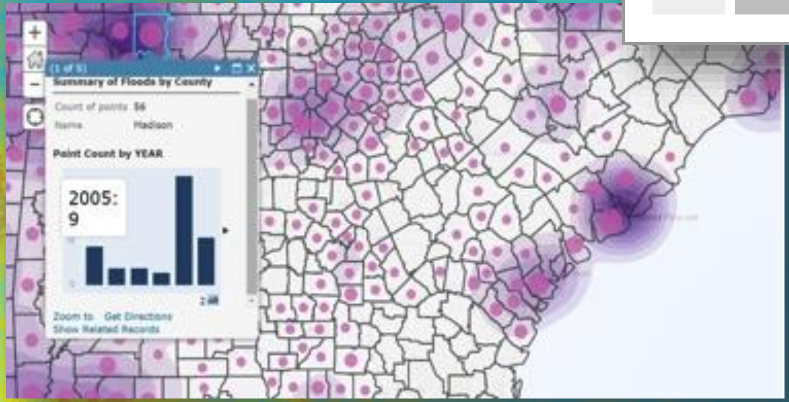
Multi-Modal Routing



Charting



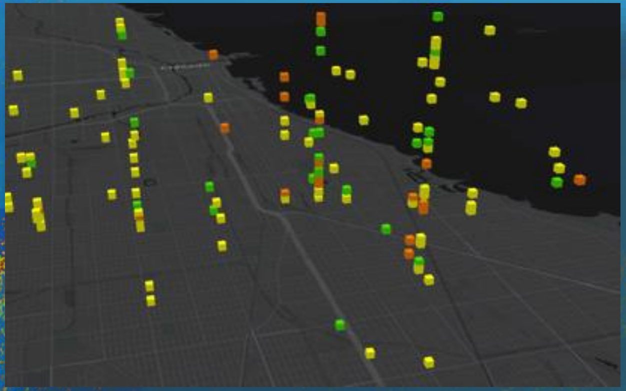
Aggregation



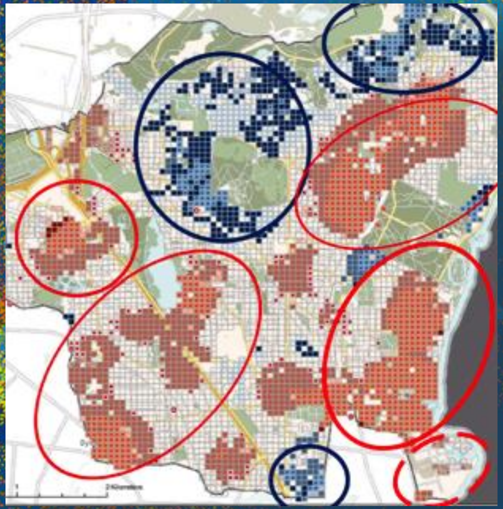
Hot Spots

Find Patterns in Time & Space

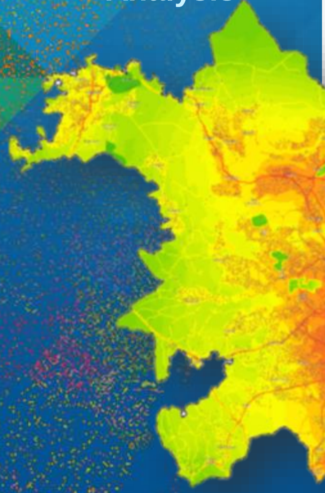
Anomaly Detection



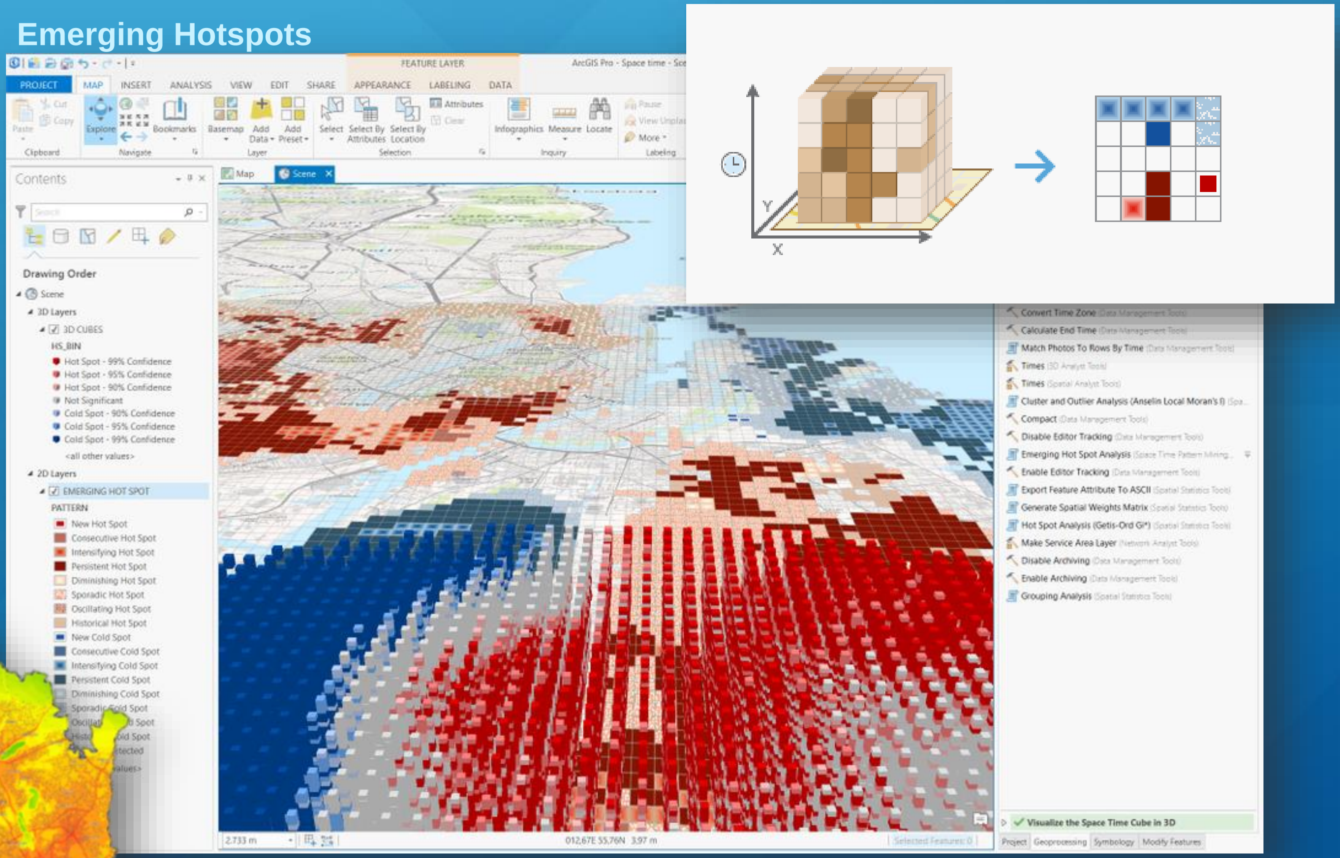
Statistical Clustering



Regression Analysis



Emerging Hotspots



PROJECT
MAP
INSERT
ANALYSIS
VIEW
EDIT
SHARE
APPEARANCE
LABELING
DATA
FEATURE LAYER
ArcGIS Pro - Space time - Sce
Paste
Cut
Copy
Clipboard
Explore
Navigate
Bookmarks
Basemap
Add Data
Add Preset
Layer
Select
Select By Attributes
Select By Location
Attributes
Clear
Selection
Infographics
Measure
Locate
Inquiry
Pause
View Unplaced
More
Labeling
Contents
Map
Scene
Drawing Order
Scene
3D Layers
3D CUBES
HS_BIN
Hot Spot - 99% Confidence
Hot Spot - 95% Confidence
Hot Spot - 90% Confidence
Not Significant
Cold Spot - 90% Confidence
Cold Spot - 95% Confidence
Cold Spot - 99% Confidence
<all other values>
2D Layers
EMERGING HOT SPOT
PATTERN
New Hot Spot
Consecutive Hot Spot
Intensifying Hot Spot
Persistent Hot Spot
Diminishing Hot Spot
Sporadic Hot Spot
Oscillating Hot Spot
Historical Hot Spot
New Cold Spot
Consecutive Cold Spot
Intensifying Cold Spot
Persistent Cold Spot
Diminishing Cold Spot
Sporadic Cold Spot
Convert Time Zone (Data Management Tools)
Calculate End Time (Data Management Tools)
Match Photos To Rows By Time (Data Management Tools)
Times (3D Analyst Tools)
Times (Spatial Analyst Tools)
Cluster and Outlier Analysis (Anselin Local Moran's I) (Spa...
Compact (Data Management Tools)
Disable Editor Tracking (Data Management Tools)
Emerging Hot Spot Analysis (Space Time Pattern Mining...
Enable Editor Tracking (Data Management Tools)
Export Feature Attribute To ASCII (Spatial Statistics Tools)
Generate Spatial Weights Matrix (Spatial Statistics Tools)
Hot Spot Analysis (Getis-Ord Gi*) (Spatial Statistics Tools)
Make Service Area Layer (Network Analyst Tools)
Disable Archiving (Data Management Tools)
Enable Archiving (Data Management Tools)
Grouping Analysis (Spatial Statistics Tools)
✓ Visualize the Space Time Cube in 3D
Project
Geoprocessing
Symbology
Modify Features
2,733 m
Y
X

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

- What are the impacts to your mission, operations, or business activities from Sensor Alarms, IT outages or impairments, or Cyber Security events?

- How do you prioritize the work of your Maintenance, IT Team or Cyber Security Team in the context of your most important missions, operations, or business activities?

- How do you provide Shared Situational Awareness across your organization?

Sensor and Cyberspace Re-Considered

It's Mappable

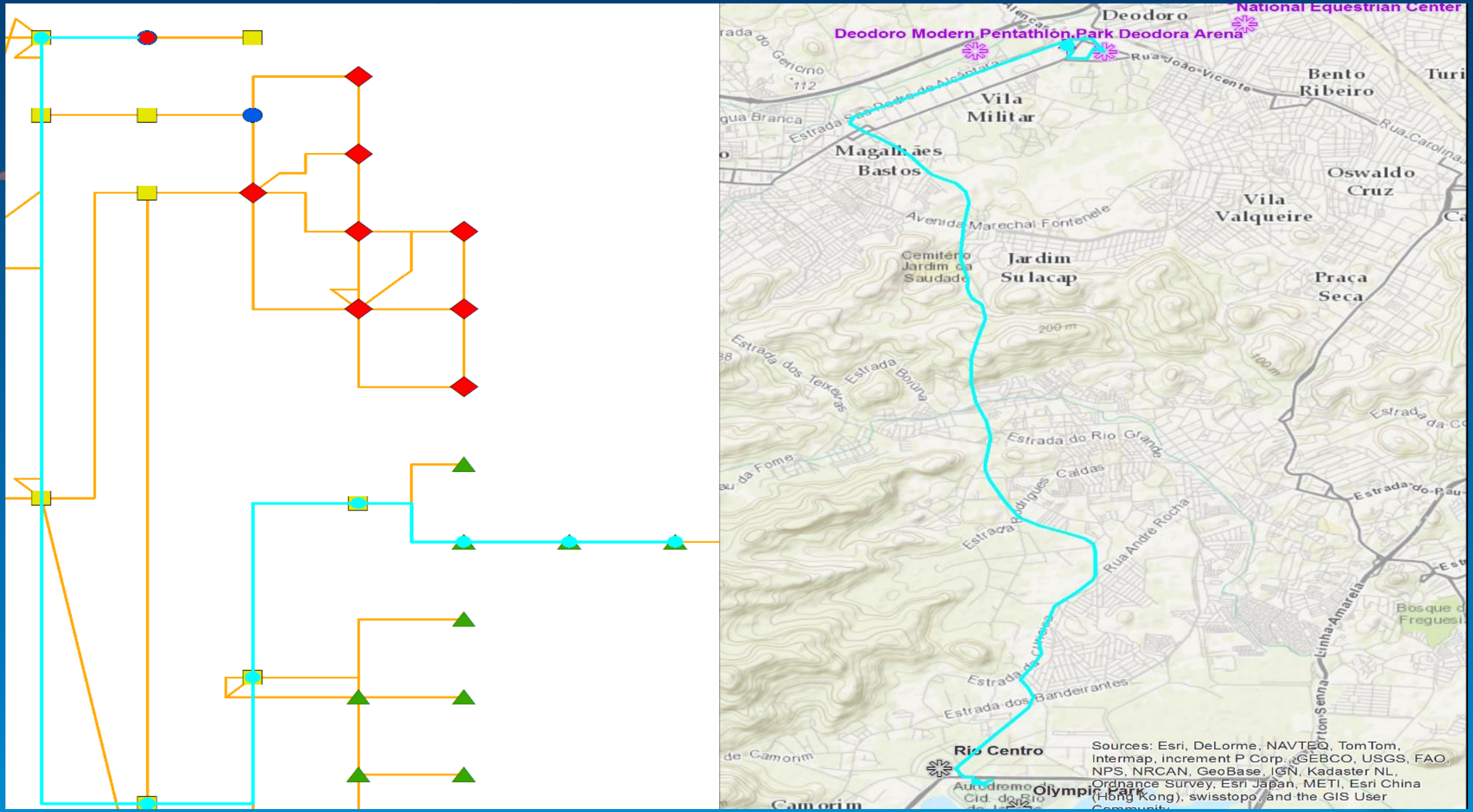
Social / Persona Layer

Sensor/Device Layer

Logical Network Layer

Physical Network Layer

Geographic Layer

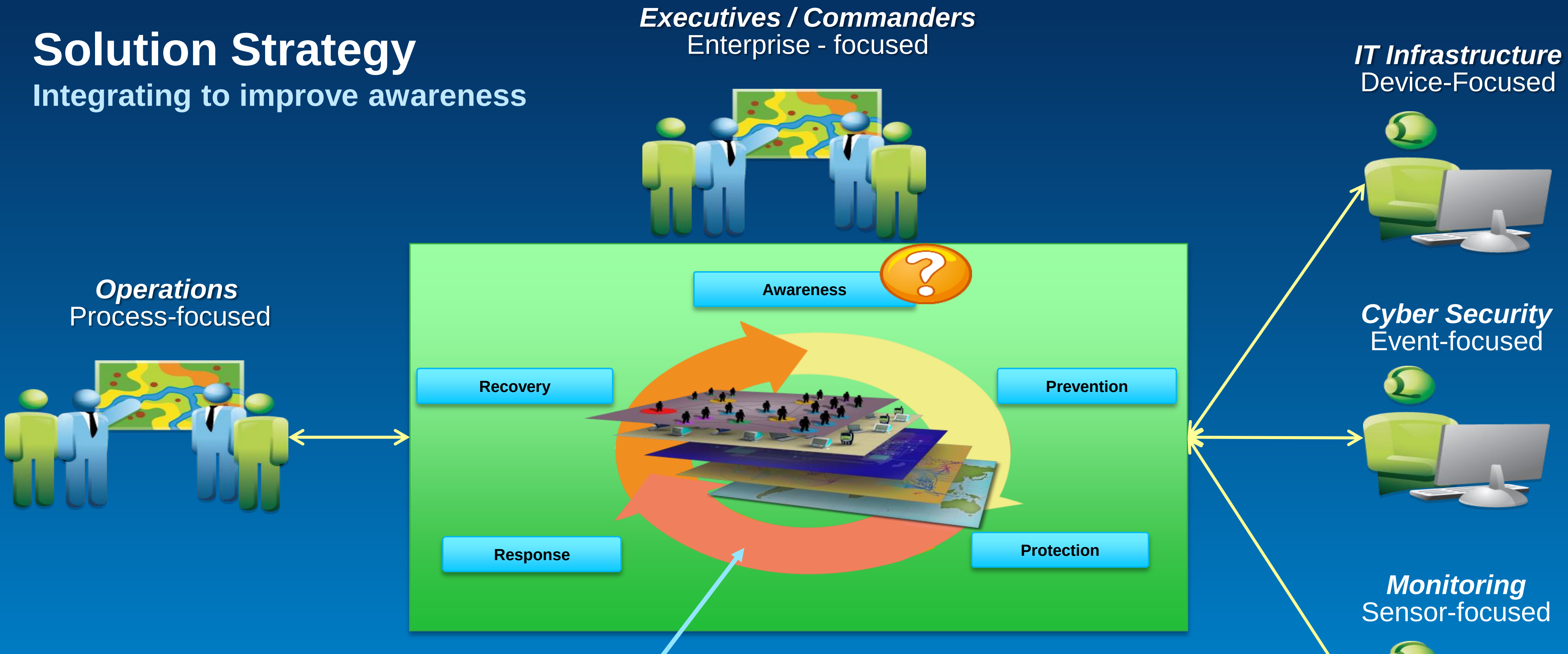


Sources: Esri, DeLorme, NAVTEQ, TomTom, Intermap, increment P Corp., GEBCO, USGS, FAO, NPS, NRCAN, GeoBase, IGN, Kadaster NL, Ordnance Survey, Esri Japan, METI, Esri China (Hong Kong), swisstopo, and the GIS User Community

- Each sensor/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

Solution Strategy

Integrating to improve awareness



Executives / Commanders
Enterprise - focused

Operations
Process-focused

IT Infrastructure
Device-Focused

Cyber Security
Event-focused

Monitoring
Sensor-focused

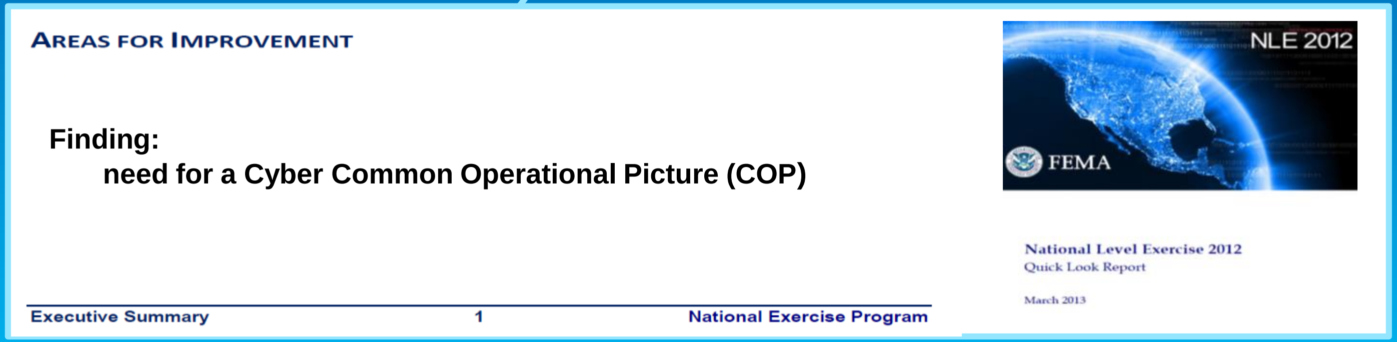
Awareness

Recovery

Prevention

Response

Protection



Areas for Improvement

Finding:
need for a Cyber Common Operational Picture (COP)

Executive Summary 1 National Exercise Program

NLE 2012

FEMA

National Level Exercise 2012
Quick Look Report

March 2013

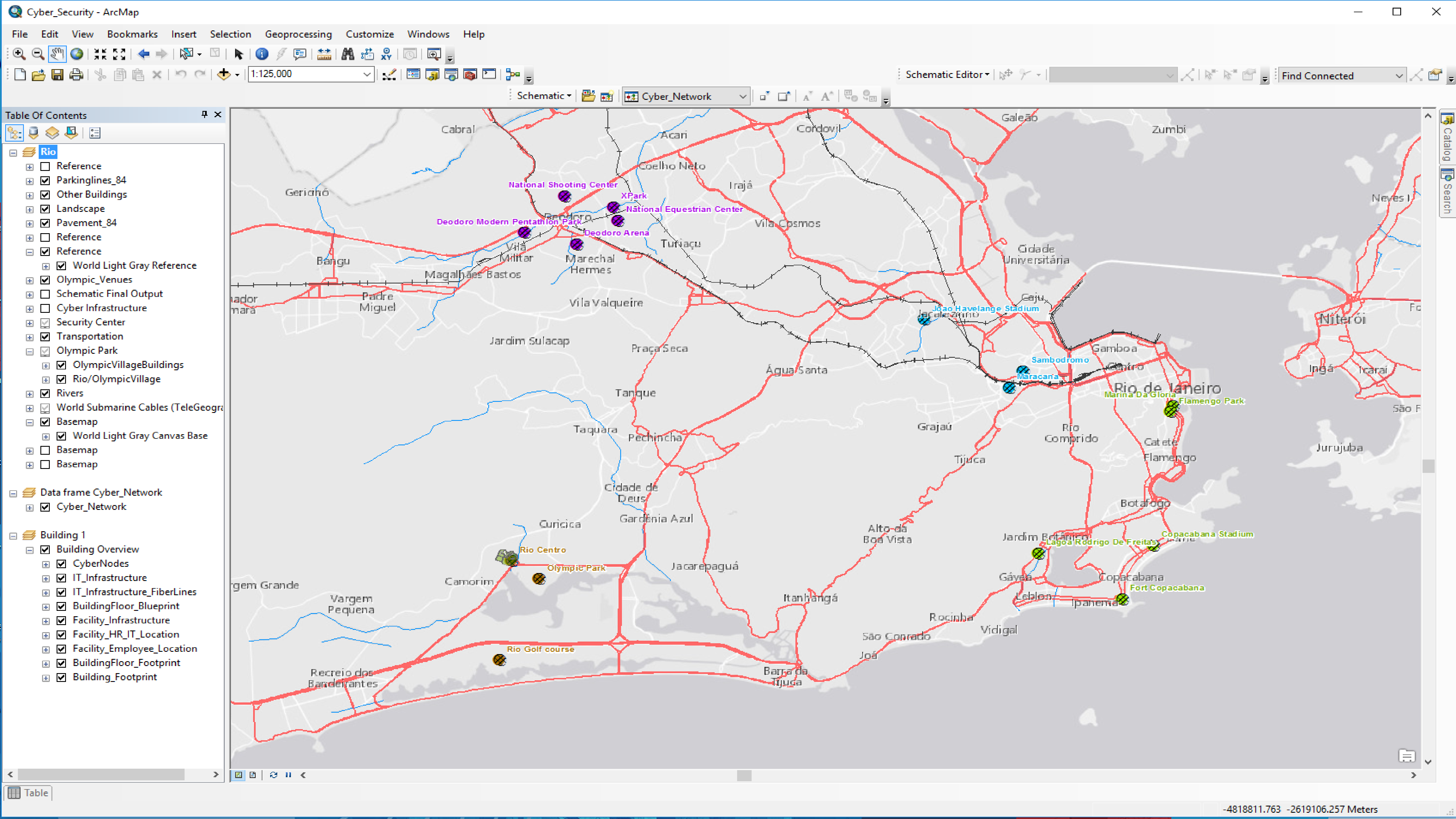
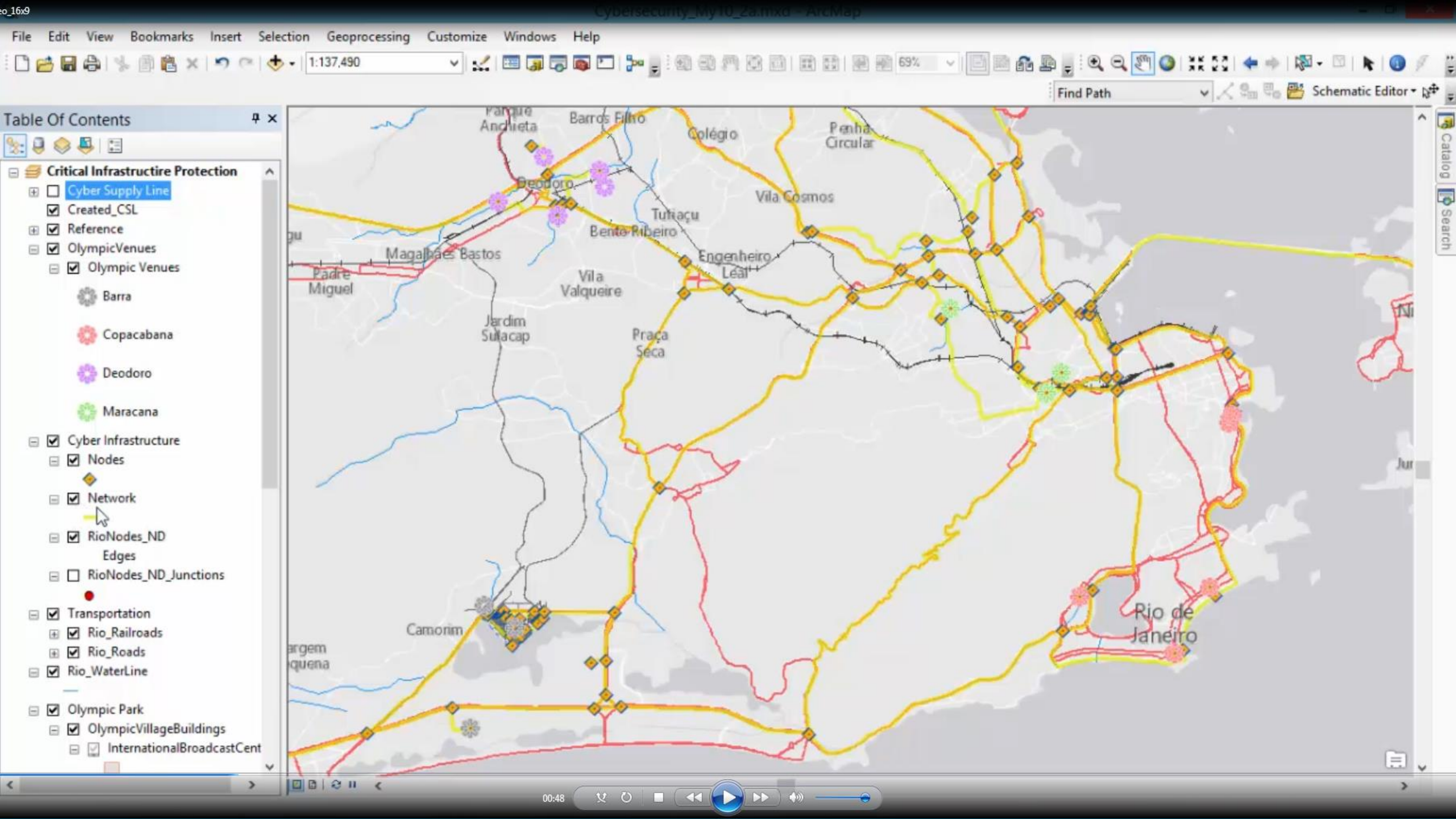


Table Of Contents

- ⊟ Rio
  - ⊞ □ Reference
  - ⊞ ☑ Parkinglines_84
  - ⊞ ☑ Other Buildings
  - ⊞ ☑ Landscape
  - ⊞ ☑ Pavement_84
  - ⊞ □ Reference
  - ⊟ ☑ Reference
    - ⊞ ☑ World Light Gray Reference
  - ⊞ ☑ Olympic_Venues
  - ⊞ □ Schematic Final Output
  - ⊞ □ Cyber Infrastructure
  - ⊞ ☑ Security Center
  - ⊞ ☑ Transportation
  - ⊟ ☑ Olympic Park
    - ⊞ ☑ OlympicVillageBuildings
    - ⊞ ☑ Rio/OlympicVillage
  - ⊞ ☑ Rivers
  - ⊞ ☑ World Submarine Cables (TeleGeogra
  - ⊟ ☑ Basemap
    - ⊞ ☑ World Light Gray Canvas Base
  - ⊞ □ Basemap
  - ⊞ □ Basemap
- ⊟ Data frame Cyber_Network
  - ⊞ ☑ Cyber_Network
- ⊟ Building 1
  - ⊟ ☑ Building Overview
    - ⊞ ☑ CyberNodes
    - ⊞ ☑ IT_Infrastructure
    - ⊞ ☑ IT_Infrastructure_FiberLines
    - ⊞ ☑ BuildingFloor_Blueprint
    - ⊞ ☑ Facility_Infrastructure
    - ⊞ ☑ Facility_HR_IT_Location
    - ⊞ ☑ Facility_Employee_Location
    - ⊞ ☑ BuildingFloor_Footprint
    - ⊞ ☑ Building_Footprint

-4818811.763 -2619106.257 Meters


eo_16x9
Cybersecurity_My10_2a.mxd - ArcMap
File
Edit
View
Bookmarks
Insert
Selection
Geoprocessing
Customize
Windows
Help
1:137,490
69%
Find Path
Schematic Editor
Table Of Contents
Critical Infrastructire Protection
☐ Cyber Supply Line
☑ Created_CSL
☑ Reference
☑ OlympicVenues
☑ Olympic Venues
Barra
Copacabana
Deodoro
Maracana
☑ Cyber Infrastructure
☑ Nodes
☑ Network
☑ RioNodes_ND
Edges
☐ RioNodes_ND_Junctions
☑ Transportation
☑ Rio_Railroads
☑ Rio_Roads
☑ Rio_WaterLine
☑ Olympic Park
☑ OlympicVillageBuildings
InternationalBroadcastCent
Parque Anchieta
Barros Filho
Colégio
Penha Circular
Deodoro
Vila Cosmos
Tuiiaçu
Bento Ribeiro
Magalhães Bastos
Engenheiro Leal
Padre Miguel
Vila Valqueire
Jardim Sulacap
Praça Seca
Camorim
Rio de Janeiro
Catalog
Search
00:48

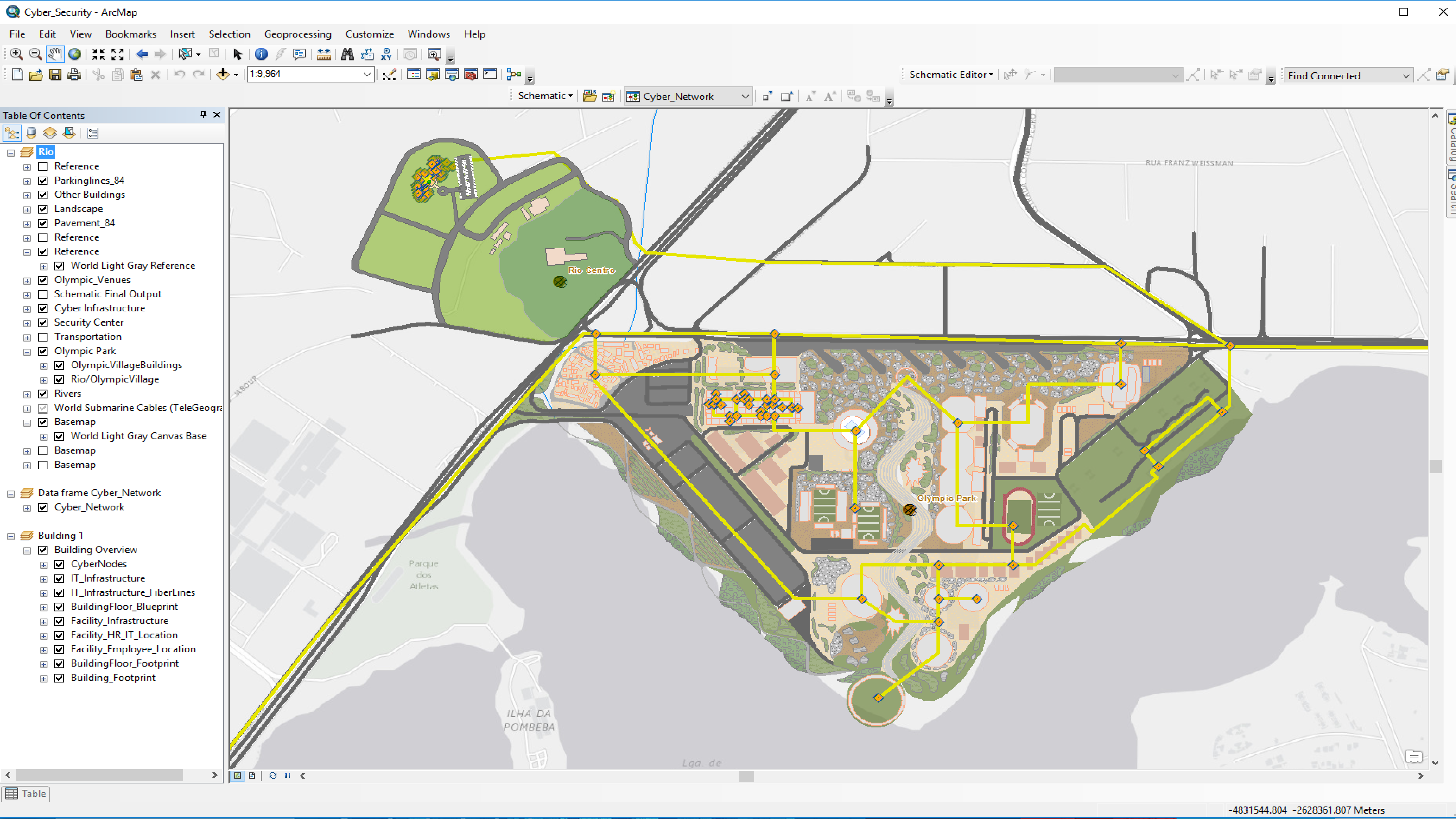
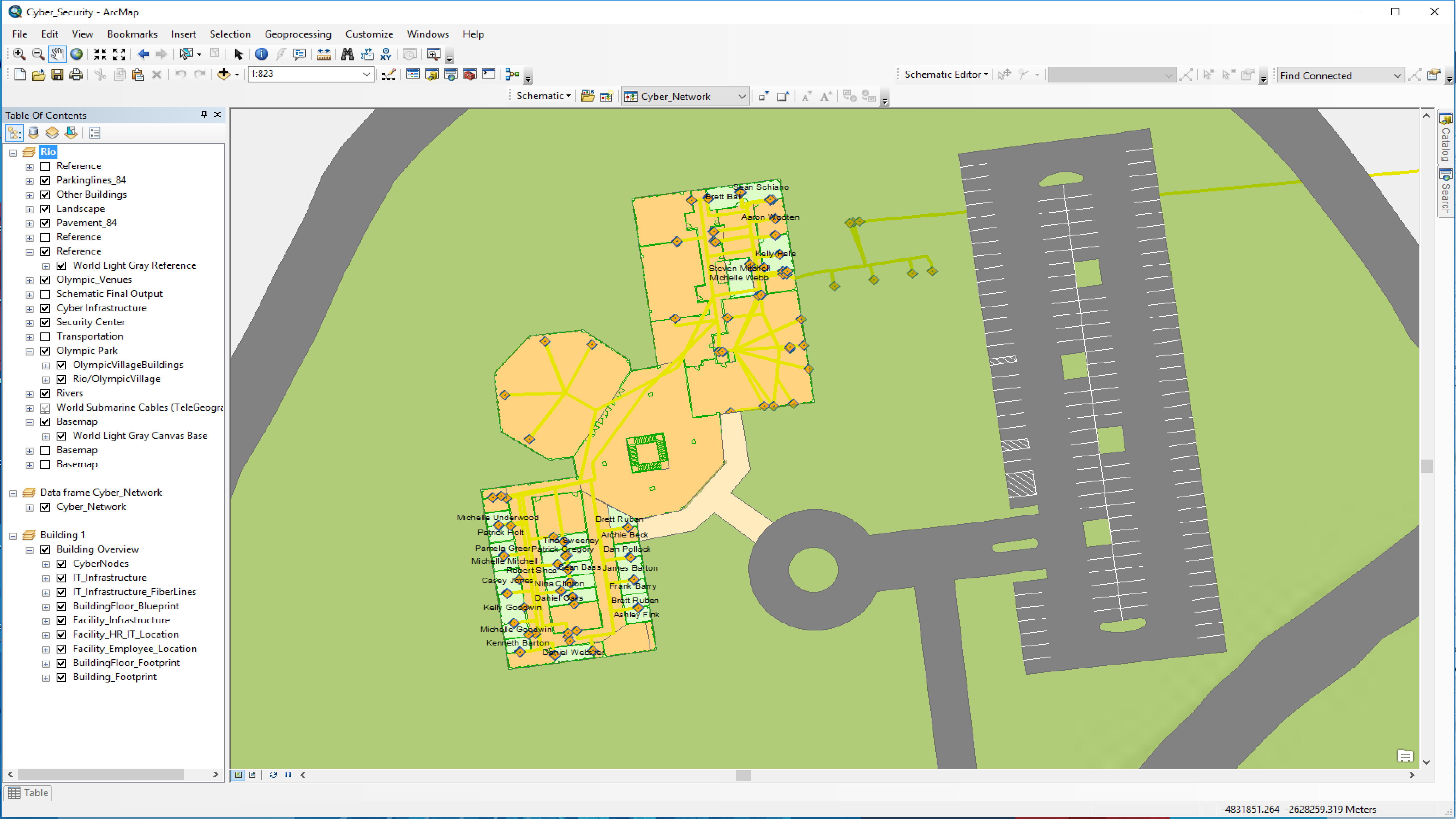


Table Of Contents

- Rio
  - ☐ Reference
  - ☑ Parkinglines_84
  - ☑ Other Buildings
  - ☑ Landscape
  - ☑ Pavement_84
  - ☐ Reference
  - ☑ Reference
    - ☑ World Light Gray Reference
  - ☑ Olympic_Venues
  - ☐ Schematic Final Output
  - ☑ Cyber Infrastructure
  - ☑ Security Center
  - ☐ Transportation
  - ☑ Olympic Park
    - ☑ OlympicVillageBuildings
    - ☑ Rio/OlympicVillage
  - ☑ Rivers
  - ☑ World Submarine Cables (TeleGeogra
  - ☑ Basemap
    - ☑ World Light Gray Canvas Base
  - ☐ Basemap
  - ☐ Basemap
- Data frame Cyber_Network
  - ☑ Cyber_Network
- Building 1
  - ☑ Building Overview
    - ☑ CyberNodes
    - ☑ IT_Infrastructure
    - ☑ IT_Infrastructure_FiberLines
    - ☑ BuildingFloor_Blueprint
    - ☑ Facility_Infrastructure
    - ☑ Facility_HR_IT_Location
    - ☑ Facility_Employee_Location
    - ☑ BuildingFloor_Footprint
    - ☑ Building_Footprint

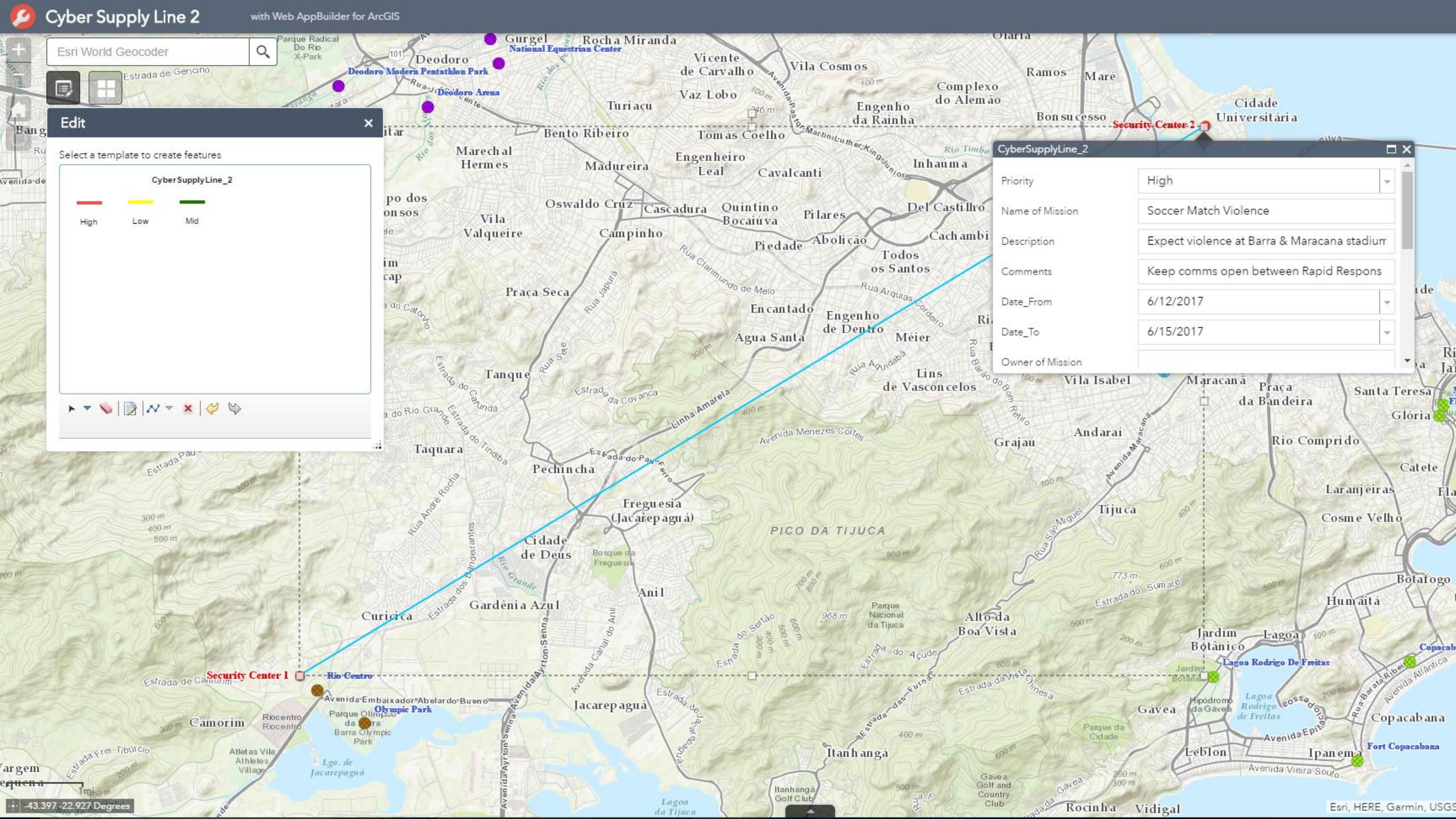


Cyber_Security - ArcMap

Table Of Contents

- ⊟ Rio
  - ⊞ □ Reference
  - ⊞ ☑ Parkinglines_84
  - ⊞ ☑ Other Buildings
  - ⊞ ☑ Landscape
  - ⊞ ☑ Pavement_84
  - ⊞ □ Reference
  - ⊟ ☑ Reference
    - ⊞ ☑ World Light Gray Reference
  - ⊞ ☑ Olympic_Venues
  - ⊞ □ Schematic Final Output
  - ⊞ ☑ Cyber Infrastructure
  - ⊞ ☑ Security Center
  - ⊞ □ Transportation
  - ⊟ ☑ Olympic Park
    - ⊞ ☑ OlympicVillageBuildings
    - ⊞ ☑ Rio/OlympicVillage
  - ⊞ ☑ Rivers
  - ⊞ ☑ World Submarine Cables (TeleGeogra
  - ⊟ ☑ Basemap
    - ⊞ ☑ World Light Gray Canvas Base
  - ⊞ □ Basemap
  - ⊞ □ Basemap
- ⊟ Data frame Cyber_Network
  - ⊞ ☑ Cyber_Network
- ⊟ Building 1
  - ⊟ ☑ Building Overview
    - ⊞ ☑ CyberNodes
    - ⊞ ☑ IT_Infrastructure
    - ⊞ ☑ IT_Infrastructure_FiberLines
    - ⊞ ☑ BuildingFloor_Blueprint
    - ⊞ ☑ Facility_Infrastructure
    - ⊞ ☑ Facility_HR_IT_Location
    - ⊞ ☑ Facility_Employee_Location
    - ⊞ ☑ BuildingFloor_Footprint
    - ⊞ ☑ Building_Footprint

-4831851.264 -2628259.319 Meters



Cyber Supply Line 2

with Web AppBuilder for ArcGIS

Esri World Geocoder

Edit

Select a template to create features

CyberSupplyLine_2

High	Low	Mid

CyberSupplyLine_2

Priority	High
Name of Mission	Soccer Match Violence
Description	Expect violence at Barra & Maracana stadiurr
Comments	Keep comms open between Rapid Respons
Date_From	6/12/2017
Date_To	6/15/2017
Owner of Mission	

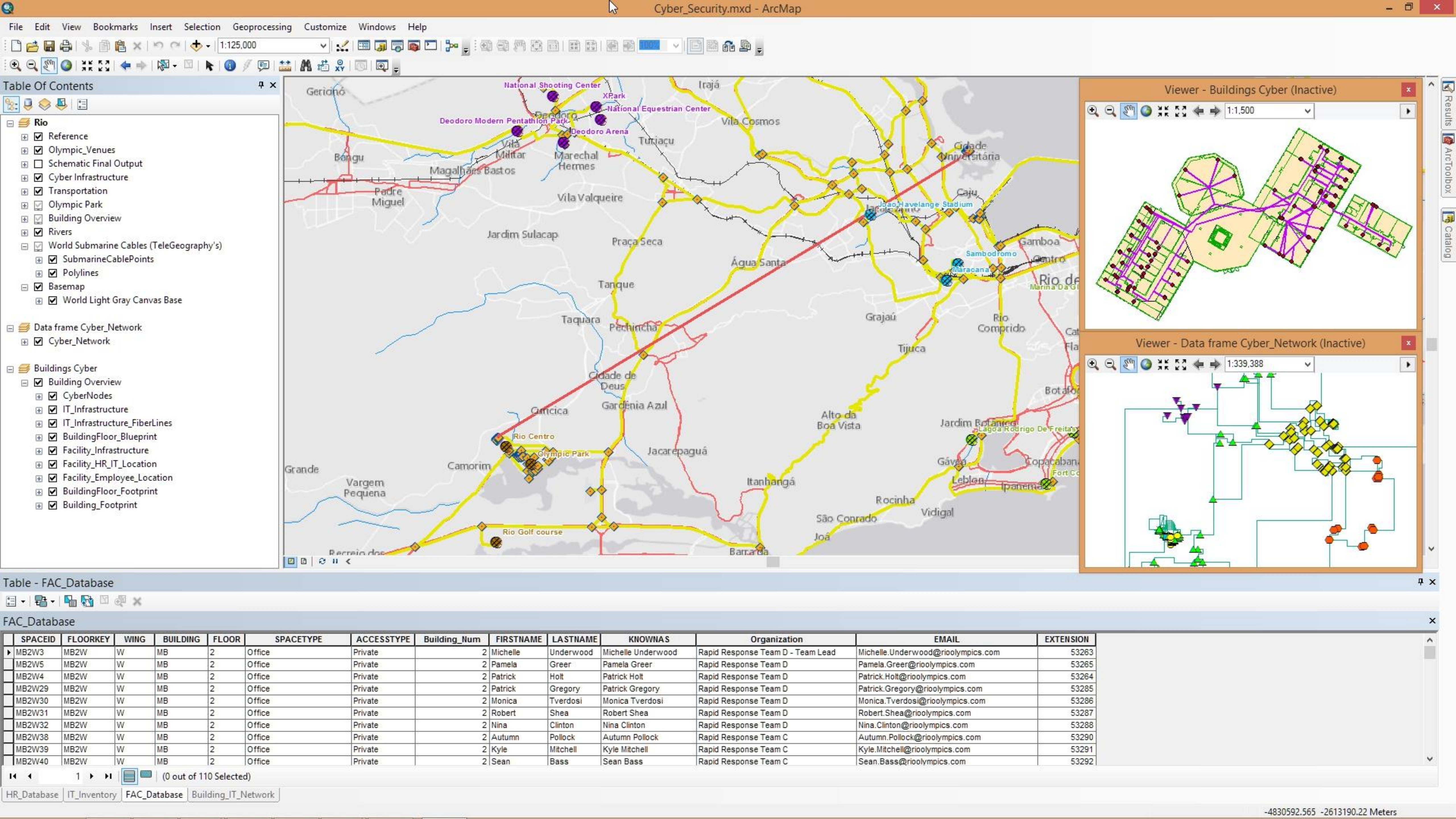


Table Of Contents

- Rio
  - ☑ Reference
  - ☑ Olympic_Venues
  - □ Schematic Final Output
  - ☑ Cyber Infrastructure
  - ☑ Transportation
  - ☑ Olympic Park
  - ☑ Building Overview
  - ☑ Rivers
  - ☑ World Submarine Cables (TeleGeography's)
    - ☑ SubmarineCablePoints
    - ☑ Polylines
  - ☑ Basemap
    - ☑ World Light Gray Canvas Base
- Data frame Cyber_Network
  - ☑ Cyber_Network
- Buildings Cyber
  - ☑ Building Overview
    - ☑ CyberNodes
    - ☑ IT_Infrastructure
    - ☑ IT_Infrastructure_FiberLines
    - ☑ BuildingFloor_Blueprint
    - ☑ Facility_Infrastructure
    - ☑ Facility_HR_IT_Location
    - ☑ Facility_Employee_Location
    - ☑ BuildingFloor_Footprint
    - ☑ Building_Footprint

Table - FAC_Database

FAC_Database

SPACEID	FLOORKEY	WING	BUILDING	FLOOR	SPACETYPE	ACCESSTYPE	Building_Num	FIRSTNAME	LASTNAME	KNOWNAS	Organization	EMAIL	EXTENSION
MB2W3	MB2W	W	MB	2	Office	Private	2	Michelle	Underwood	Michelle Underwood	Rapid Response Team D - Team Lead	Michelle.Underwood@rioolympics.com	53263
MB2W5	MB2W	W	MB	2	Office	Private	2	Pamela	Greer	Pamela Greer	Rapid Response Team D	Pamela.Greer@rioolympics.com	53265
MB2W4	MB2W	W	MB	2	Office	Private	2	Patrick	Holt	Patrick Holt	Rapid Response Team D	Patrick.Holt@rioolympics.com	53264
MB2W29	MB2W	W	MB	2	Office	Private	2	Patrick	Gregory	Patrick Gregory	Rapid Response Team D	Patrick.Gregory@rioolympics.com	53285
MB2W30	MB2W	W	MB	2	Office	Private	2	Monica	Tverdosi	Monica Tverdosi	Rapid Response Team D	Monica.Tverdosi@rioolympics.com	53286
MB2W31	MB2W	W	MB	2	Office	Private	2	Robert	Shea	Robert Shea	Rapid Response Team D	Robert.Shea@rioolympics.com	53287
MB2W32	MB2W	W	MB	2	Office	Private	2	Nina	Clinton	Nina Clinton	Rapid Response Team D	Nina.Clinton@rioolympics.com	53288
MB2W38	MB2W	W	MB	2	Office	Private	2	Autumn	Pollock	Autumn Pollock	Rapid Response Team C	Autumn.Pollock@rioolympics.com	53290
MB2W39	MB2W	W	MB	2	Office	Private	2	Kyle	Mitchell	Kyle Mitchell	Rapid Response Team C	Kyle.Mitchell@rioolympics.com	53291
MB2W40	MB2W	W	MB	2	Office	Private	2	Sean	Bass	Sean Bass	Rapid Response Team C	Sean.Bass@rioolympics.com	53292

1 (0 out of 110 Selected)

HR_Database | IT_Inventory | FAC_Database | Building_IT_Network

-4830592.565 -2613190.22 Meters

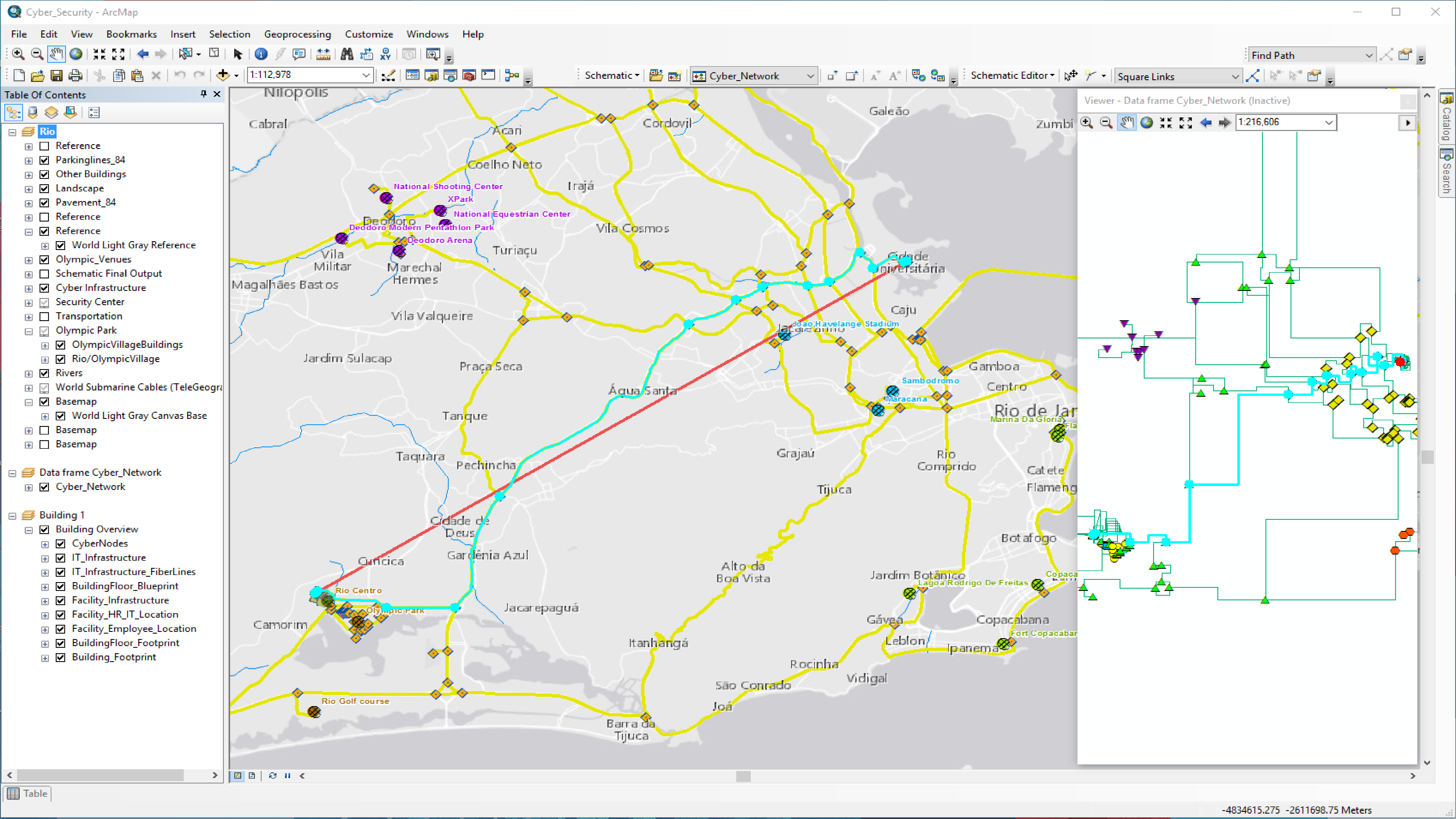
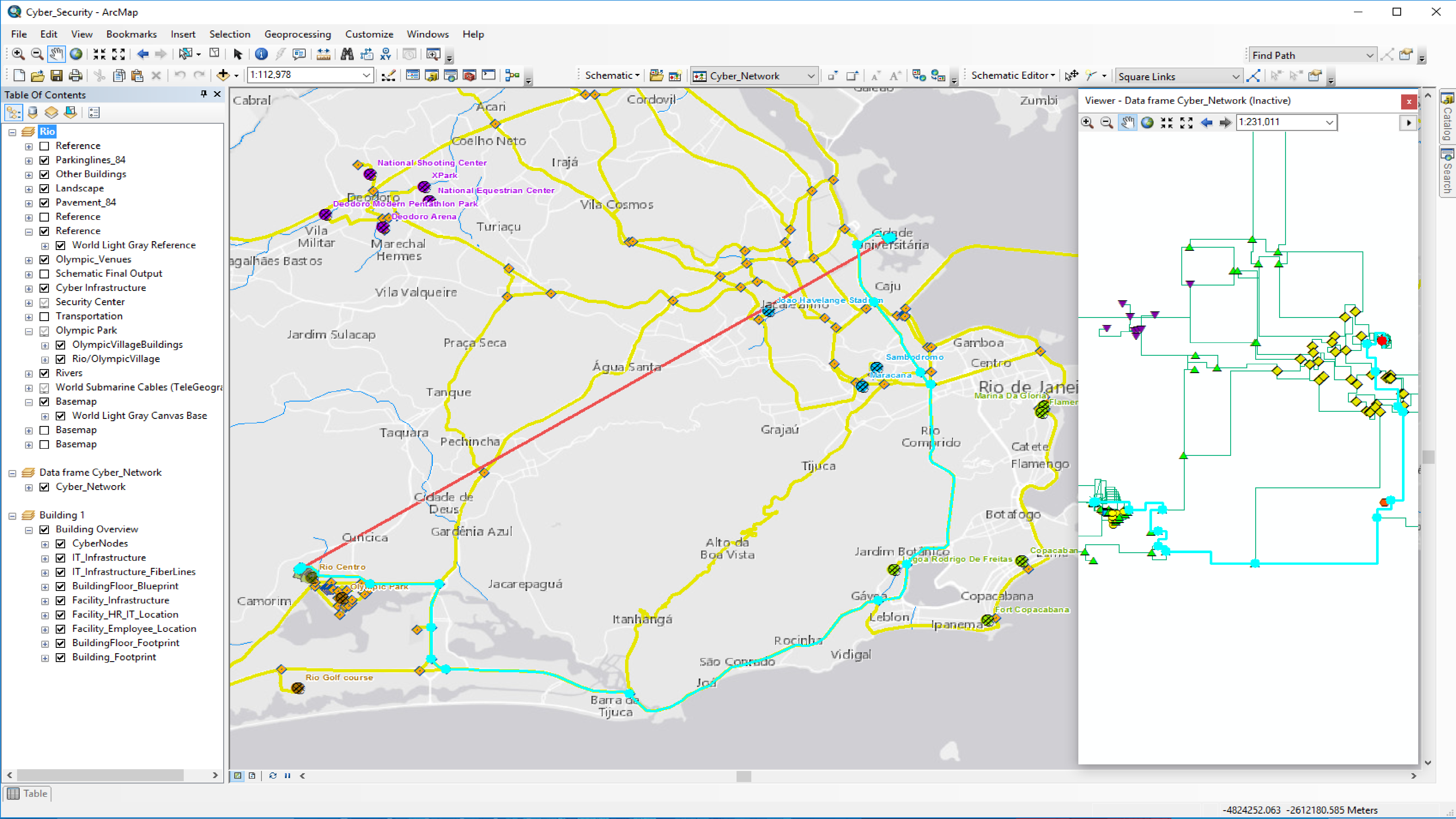


Table Of Contents

- ⊟ Rio
  - ⊞ □ Reference
  - ⊞ ☑ Parkinglines_84
  - ⊞ ☑ Other Buildings
  - ⊞ ☑ Landscape
  - ⊞ ☑ Pavement_84
  - ⊞ □ Reference
  - ⊟ ☑ Reference
    - ⊞ ☑ World Light Gray Reference
  - ⊞ ☑ Olympic_Venues
  - ⊞ □ Schematic Final Output
  - ⊞ ☑ Cyber Infrastructure
  - ⊞ ☑ Security Center
  - ⊞ □ Transportation
  - ⊟ ☑ Olympic Park
    - ⊞ ☑ OlympicVillageBuildings
    - ⊞ ☑ Rio/OlympicVillage
  - ⊞ ☑ Rivers
  - ⊞ ☑ World Submarine Cables (TeleGeogra
  - ⊟ ☑ Basemap
    - ⊞ ☑ World Light Gray Canvas Base
  - ⊞ □ Basemap
  - ⊞ □ Basemap
- ⊟ Data frame Cyber_Network
  - ⊞ ☑ Cyber_Network
- ⊟ Building 1
  - ⊟ ☑ Building Overview
    - ⊞ ☑ CyberNodes
    - ⊞ ☑ IT_Infrastructure
    - ⊞ ☑ IT_Infrastructure_FiberLines
    - ⊞ ☑ BuildingFloor_Blueprint
    - ⊞ ☑ Facility_Infrastructure
    - ⊞ ☑ Facility_HR_IT_Location
    - ⊞ ☑ Facility_Employee_Location
    - ⊞ ☑ BuildingFloor_Footprint
    - ⊞ ☑ Building_Footprint

-4834615.275 -2611698.75 Meters



Rio
- ☐ Reference
- ☑ Parkinglines_84
- ☑ Other Buildings
- ☑ Landscape
- ☑ Pavement_84
- ☐ Reference
- ☑ Reference
  - ☑ World Light Gray Reference
- ☑ Olympic_Venues
- ☐ Schematic Final Output
- ☑ Cyber Infrastructure
- ☑ Security Center
- ☐ Transportation
- ☑ Olympic Park
  - ☑ OlympicVillageBuildings
  - ☑ Rio/OlympicVillage
- ☑ Rivers
- ☑ World Submarine Cables (TeleGeogra
- ☑ Basemap
  - ☑ World Light Gray Canvas Base
- ☐ Basemap
- ☐ Basemap

Data frame Cyber_Network
- ☑ Cyber_Network

Building 1
- ☑ Building Overview
  - ☑ CyberNodes
  - ☑ IT_Infrastructure
  - ☑ IT_Infrastructure_FiberLines
  - ☑ BuildingFloor_Blueprint
  - ☑ Facility_Infrastructure
  - ☑ Facility_HR_IT_Location
  - ☑ Facility_Employee_Location
  - ☑ BuildingFloor_Footprint
  - ☑ Building_Footprint

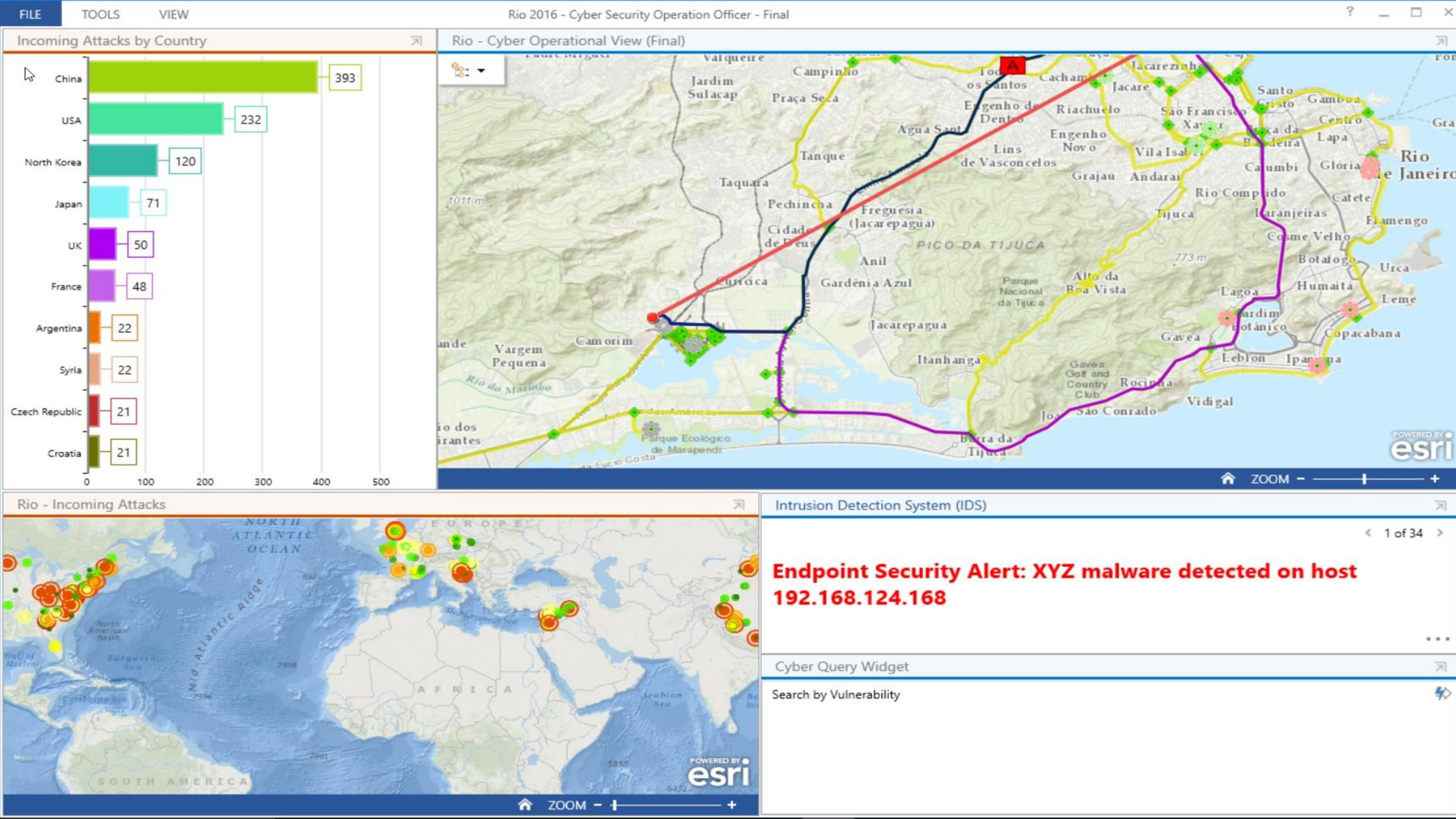
1:112,978

Cyber_Network

Square Links

1:231,011

-4824252.063 -2612180.585 Meters



Rio 2016 - Cyber Security Operation Officer - Final

Incoming Attacks by Country

Rio - Cyber Operational View (Final)

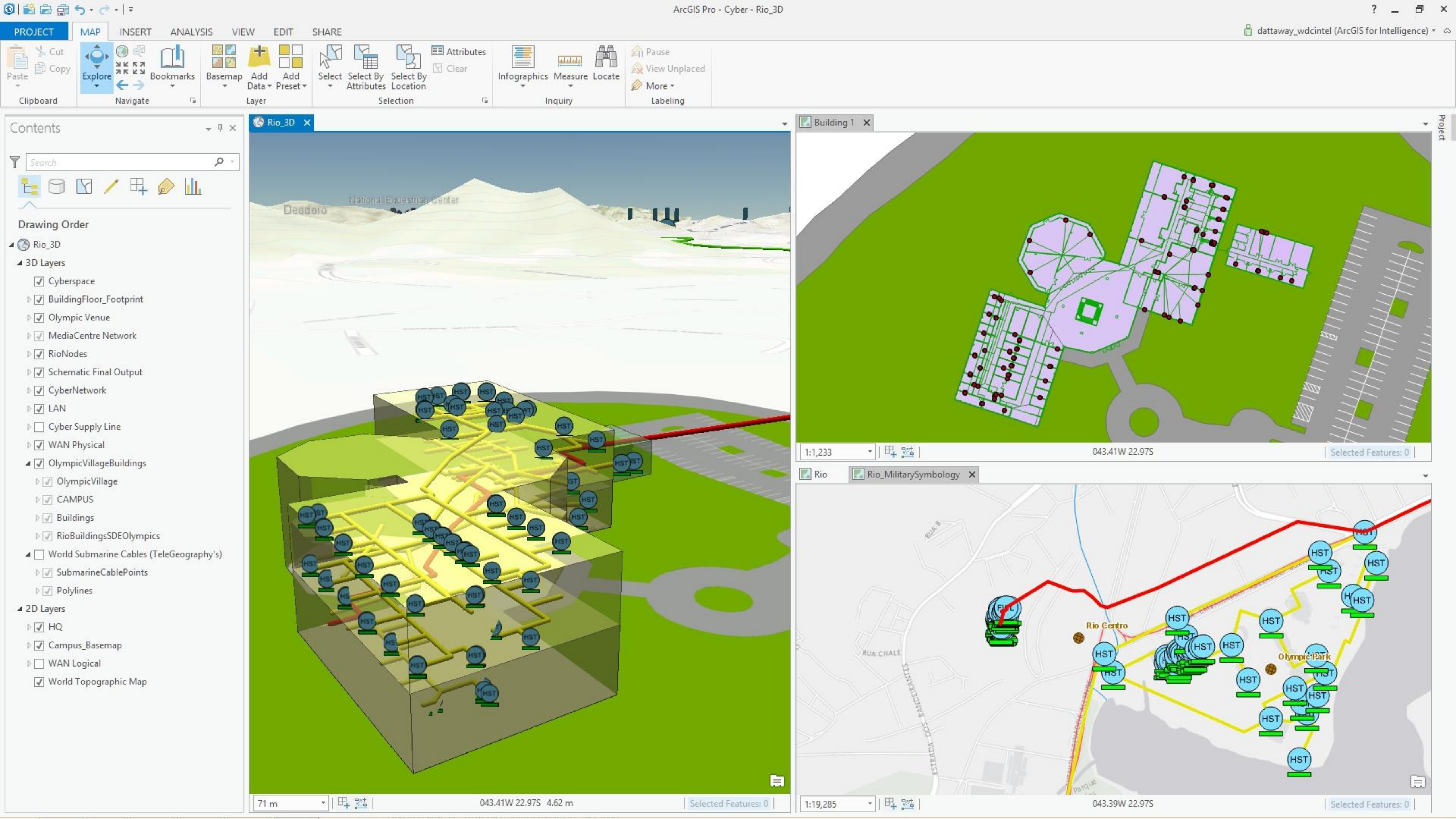
Rio - Incoming Attacks

Intrusion Detection System (IDS)

Endpoint Security Alert: XYZ malware detected on host 192.168.124.168

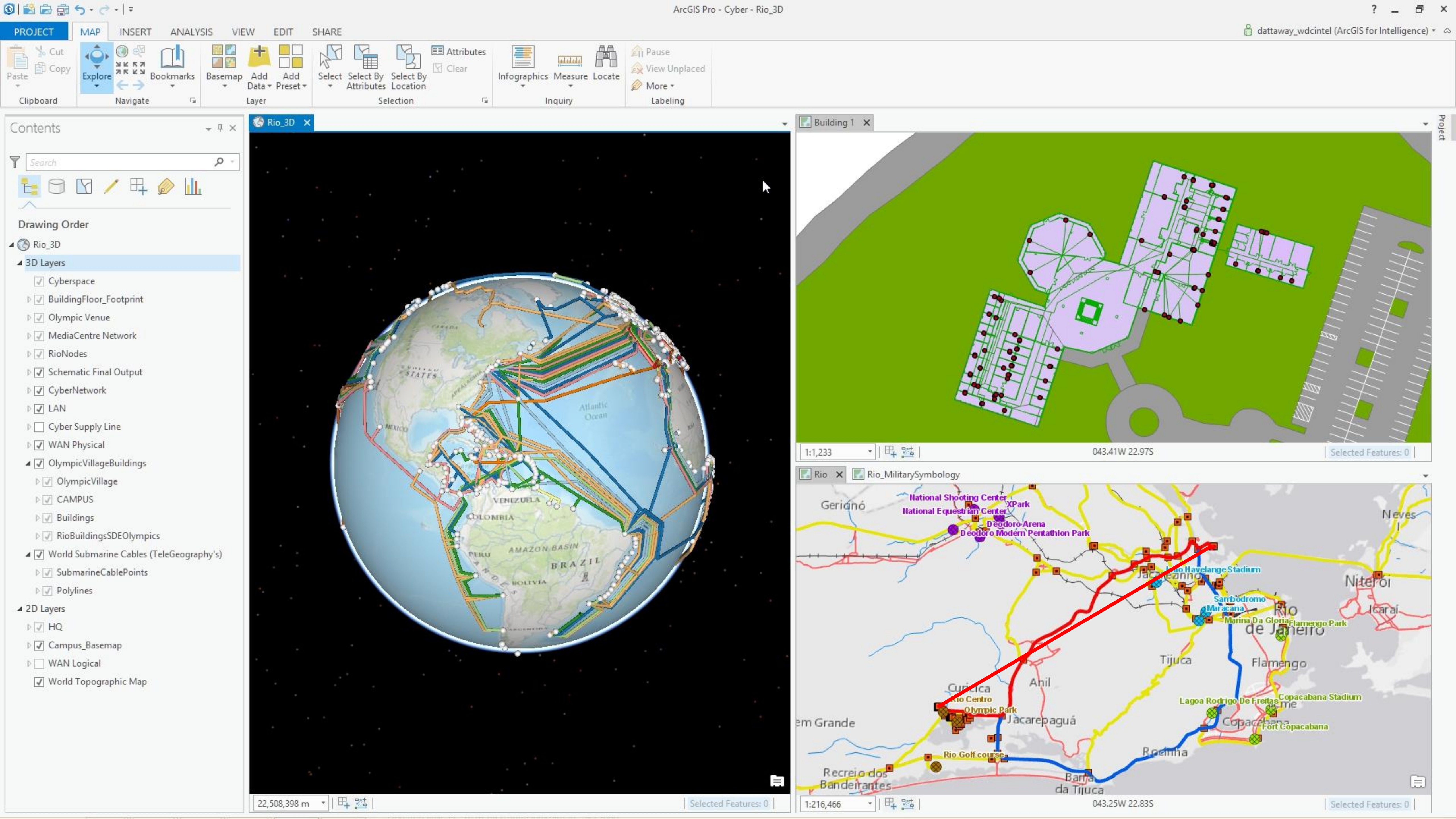
Cyber Query Widget

Search by Vulnerability



Drawing Order

- Rio_3D
  - 3D Layers
    - ☑ Cyberspace
    - ☑ BuildingFloor_Footprint
    - ☑ Olympic Venue
    - ☑ MediaCentre Network
    - ☑ RioNodes
    - ☑ Schematic Final Output
    - ☑ CyberNetwork
    - ☑ LAN
    - □ Cyber Supply Line
    - ☑ WAN Physical
    - ☑ OlympicVillageBuildings
      - ☑ OlympicVillage
      - ☑ CAMPUS
      - ☑ Buildings
      - ☑ RioBuildingsSDEOlympics
    - □ World Submarine Cables (TeleGeography's)
      - ☑ SubmarineCablePoints
      - ☑ Polylines
  - 2D Layers
    - ☑ HQ
    - ☑ Campus_Basemap
    - □ WAN Logical
    - ☑ World Topographic Map



Contents

Search

Drawing Order

- Rio_3D
  - 3D Layers
    - ☑ Cyberspace
    - ☑ BuildingFloor_Footprint
    - ☑ Olympic Venue
    - ☑ MediaCentre Network
    - ☑ RioNodes
    - ☑ Schematic Final Output
    - ☑ CyberNetwork
    - ☑ LAN
    - □ Cyber Supply Line
    - ☑ WAN Physical
    - ☑ OlympicVillageBuildings
      - ☑ OlympicVillage
      - ☑ CAMPUS
      - ☑ Buildings
      - ☑ RioBuildingsSDEOlympics
    - ☑ World Submarine Cables (TeleGeography's)
      - ☑ SubmarineCablePoints
      - ☑ Polylines
  - 2D Layers
    - ☑ HQ
    - ☑ Campus_Basemap
    - □ WAN Logical
    - ☑ World Topographic Map

ArcGIS Integration with Cyber Security Tools

Executives

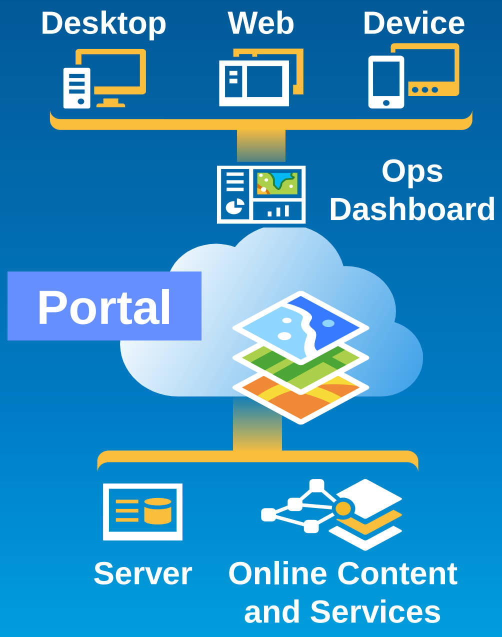
Executive Dashboards -
Status Reports, Trends,
Brand Sentiment, Financials

Operations

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

Human Resources

HR Database -
Personnel, Orgs,
Locations, Travel



Cyber Security

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

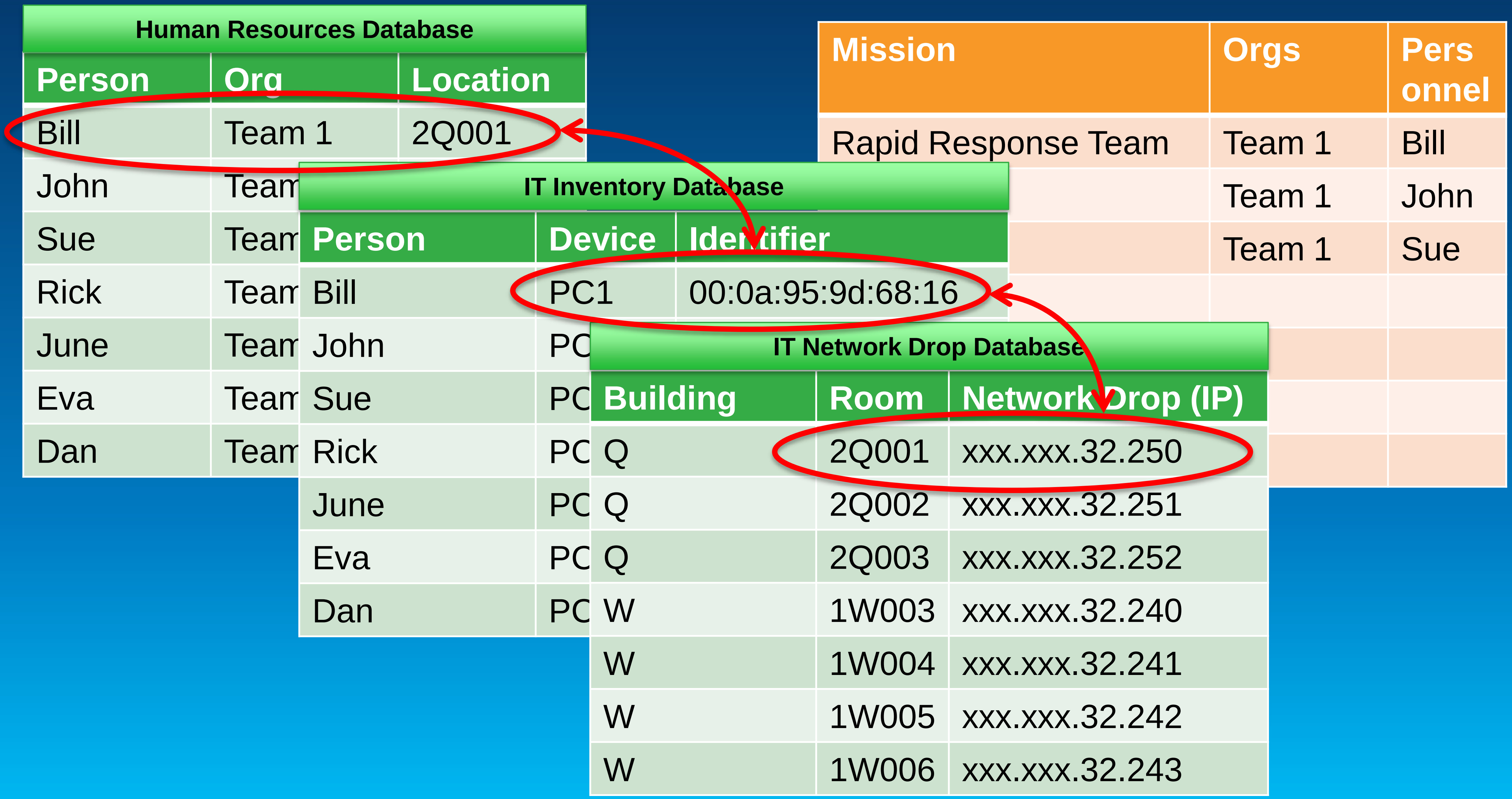
IT Operations

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

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	

Mission	Orgs	Pers onnel
Rapid Response Team	Team 1	Bill
	Team 1	John
	Team 1	Sue

IT Inventory Database

Person	Device	Identifier
Bill	PC1	00:0a:95:9d:68:16
John	PC	
Sue	PC	
Rick	PC	
June	PC	
Eva	PC	
Dan	PC	

IT Network Drop Database

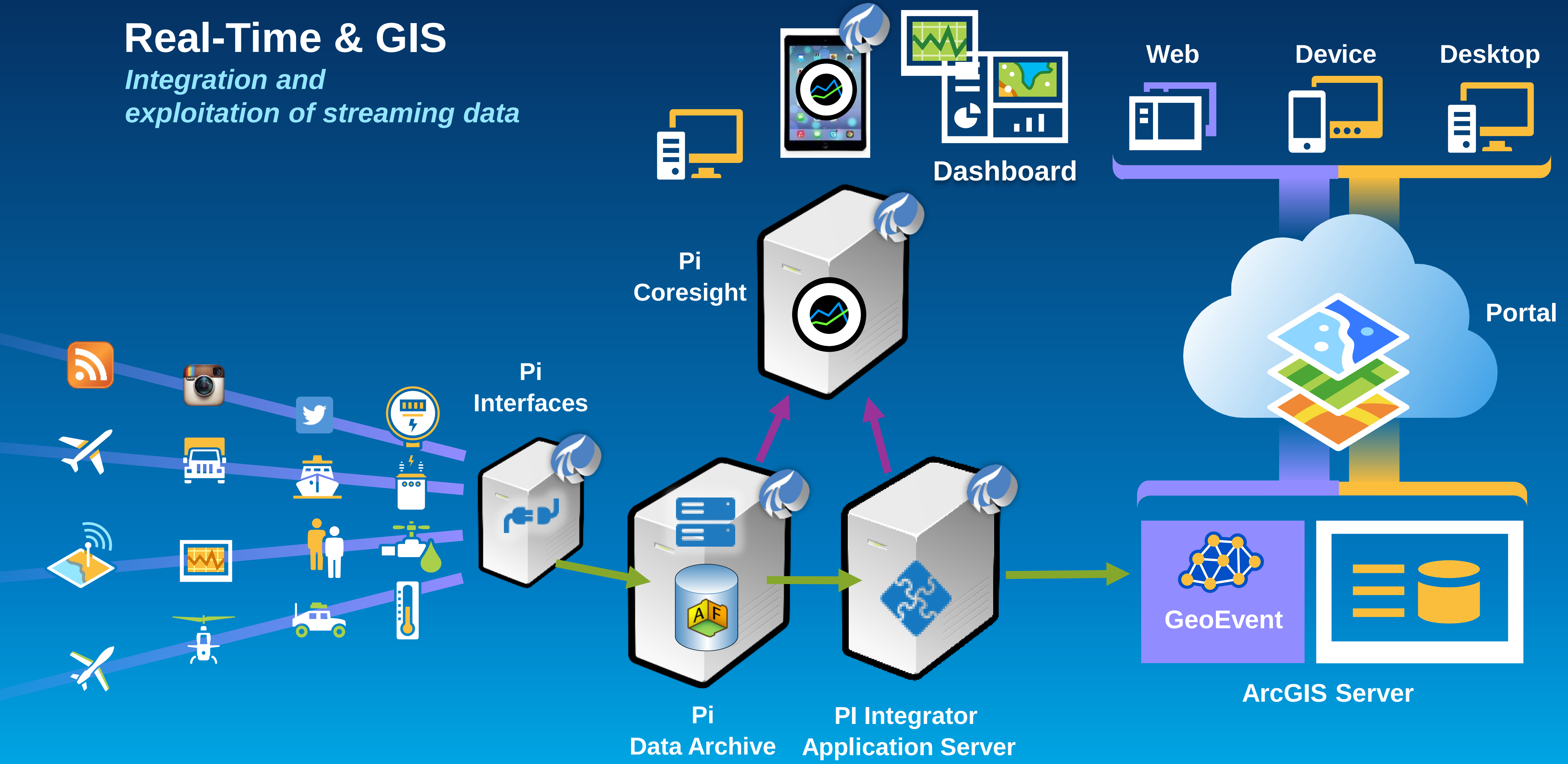
Building	Room	Network Drop (IP)
Q	2Q001	xxx.xxx.32.250
Q	2Q002	xxx.xxx.32.251
Q	2Q003	xxx.xxx.32.252
W	1W003	xxx.xxx.32.240
W	1W004	xxx.xxx.32.241
W	1W005	xxx.xxx.32.242
W	1W006	xxx.xxx.32.243

Data Linkages

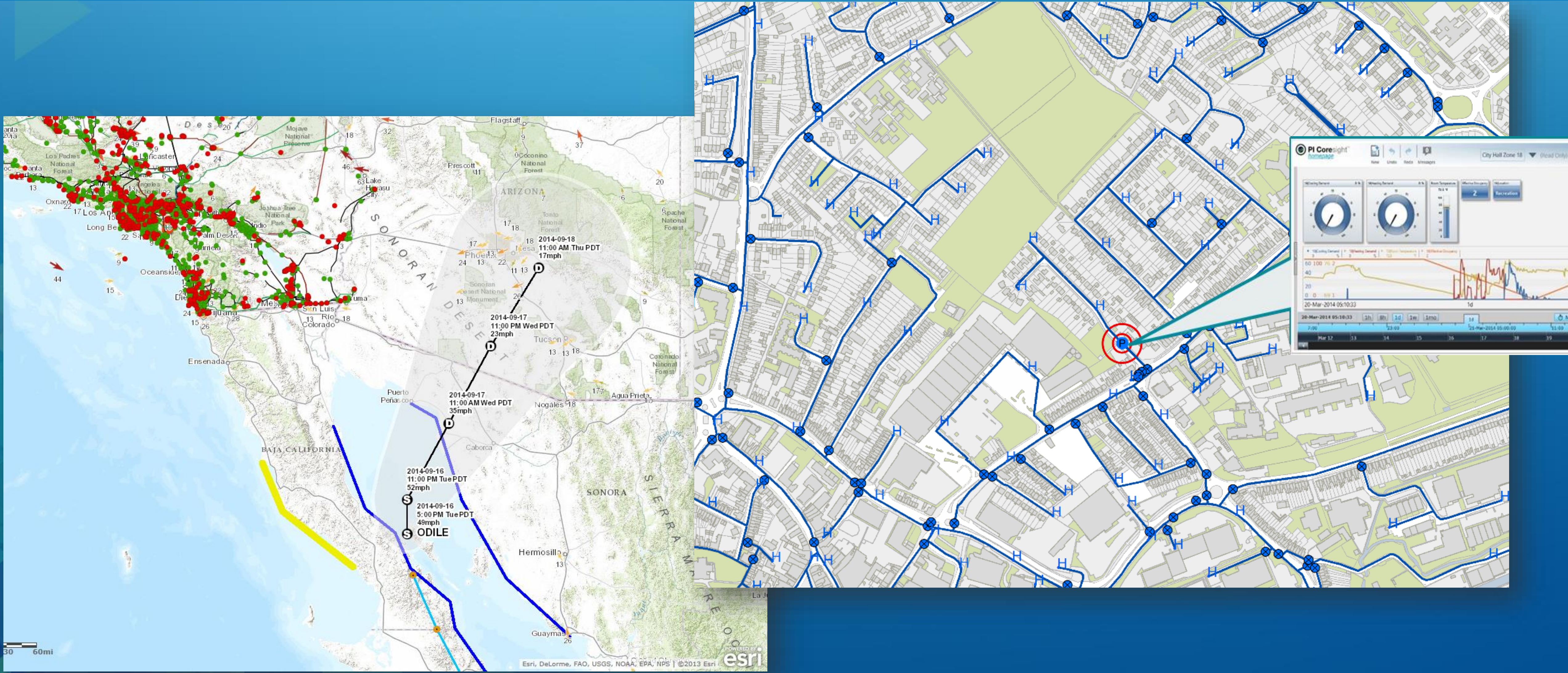
Mission / Operational activities	to	Organizations / People
Organizations	to	People
People	to	Their location
People	to	Devices they use
Systems	to	Sensors
Devices / Sensors	to	Their location
Devices / Sensors	to	Their logical network connection
Logical Network	to	Physical Network
Logical / Physical Network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

Real-Time & GIS

Integration and exploitation of streaming data

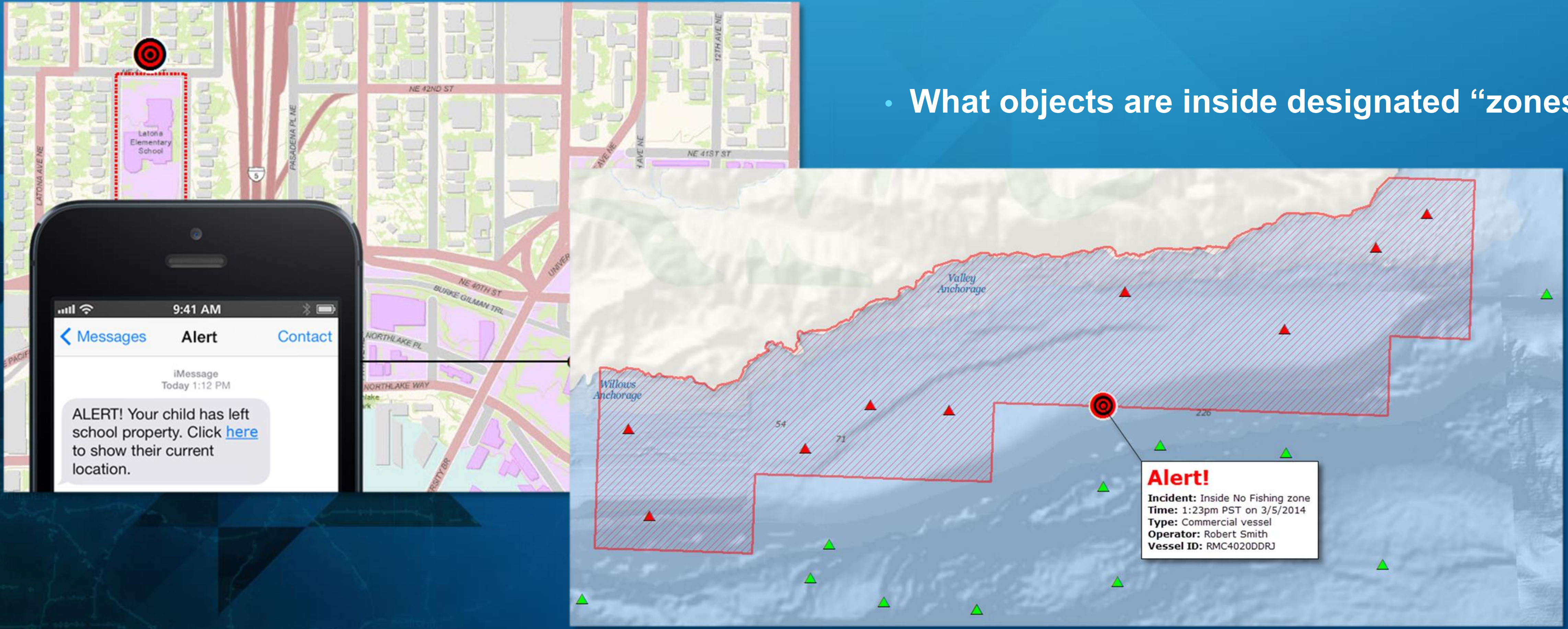


Critical Infrastructure Protection



Notifications and Alerting

- **What objects are inside designated “zones”?**



9:41 AM

Messages Alert Contact

iMessage
Today 1:12 PM

ALERT! Your child has left school property. Click here to show their current location.

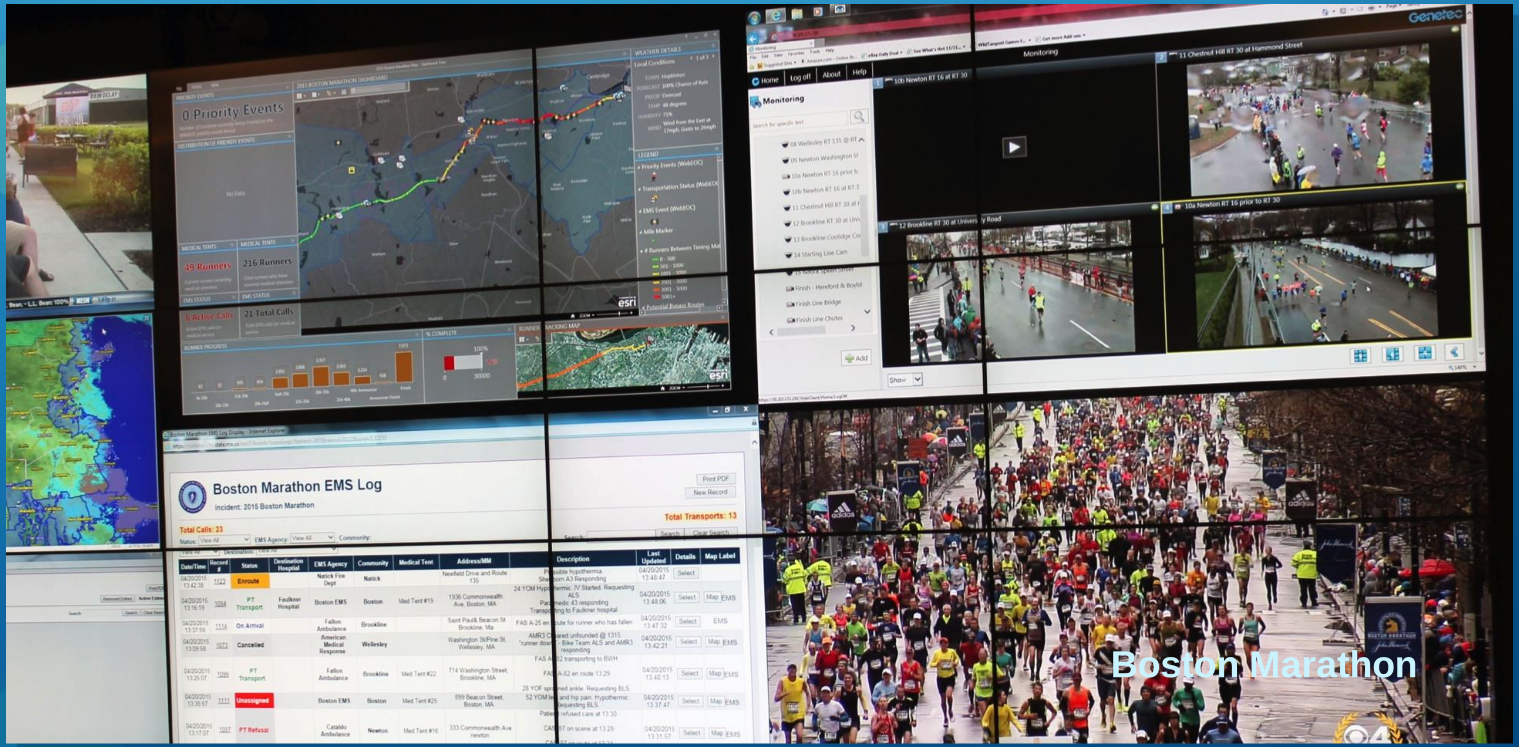
Alert!

Incident: Inside No Fishing zone
Time: 1:23pm PST on 3/5/2014
Type: Commercial vessel
Operator: Robert Smith
Vessel ID: RMC4020DDRJ

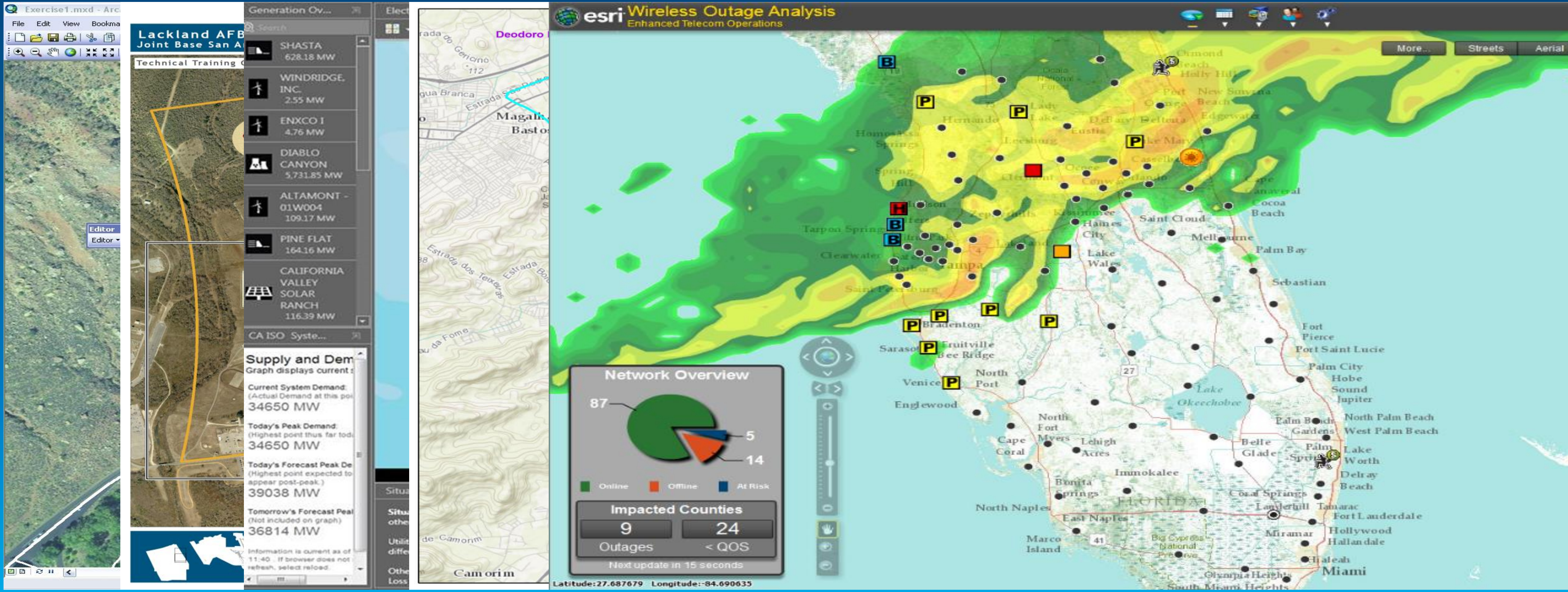
Situational Awareness

- Monitoring, Analysis and Alerting
- Stationary and Moving Events
- Large and High-Velocity Data Streams

Boston Marathon



Sensor / Cyber Summary



esri

Understanding our world.

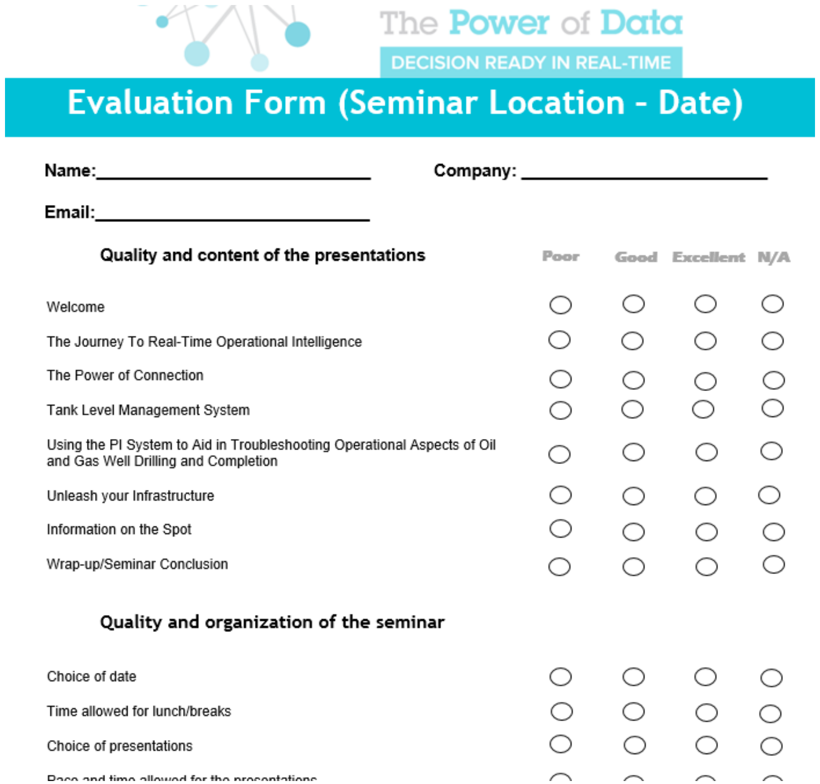
Questions

Please wait for the **microphone** before asking your questions

State your **name & organization**

Please don't forget to…

Complete the Survey for this session



The Power of Data
DECISION READY IN REAL-TIME

Evaluation Form (Seminar Location - Date)

Name:______________________ **Company:** ____________________

Email:______________________

Quality and content of the presentations	Poor	Good	Excellent	N/A
Welcome	○	○	○	○
The Journey To Real-Time Operational Intelligence	○	○	○	○
The Power of Connection	○	○	○	○
Tank Level Management System	○	○	○	○
Using the PI System to Aid in Troubleshooting Operational Aspects of Oil and Gas Well Drilling and Completion	○	○	○	○
Unleash your Infrastructure	○	○	○	○
Information on the Spot	○	○	○	○
Wrap-up/Seminar Conclusion	○	○	○	○
Quality and organization of the seminar				
Choice of date	○	○	○	○
Time allowed for lunch/breaks	○	○	○	○
Choice of presentations	○	○	○	○
Pace and time allowed for the presentations	○	○	○	○