Cybersecurity

Ken Stoni and Scott Cecilio

Problem

- **Cyber threat is becoming more prevalent**
- **Cyber threat is becoming more serious**
  - Data compromise is an existential threat to many organizations
- **The current approach to cybersecurity is device-centric & resource-intensive**
  - Protect all devices at all times
  - Organizations have insufficient resources to implement this approach
- **Organizations have legacy cybersecurity technology that can’t be abandoned**
- **It is sometimes difficult to integrate IT activities with the rest of the organization**

Cyberspace Re-Considered

It's Mappable

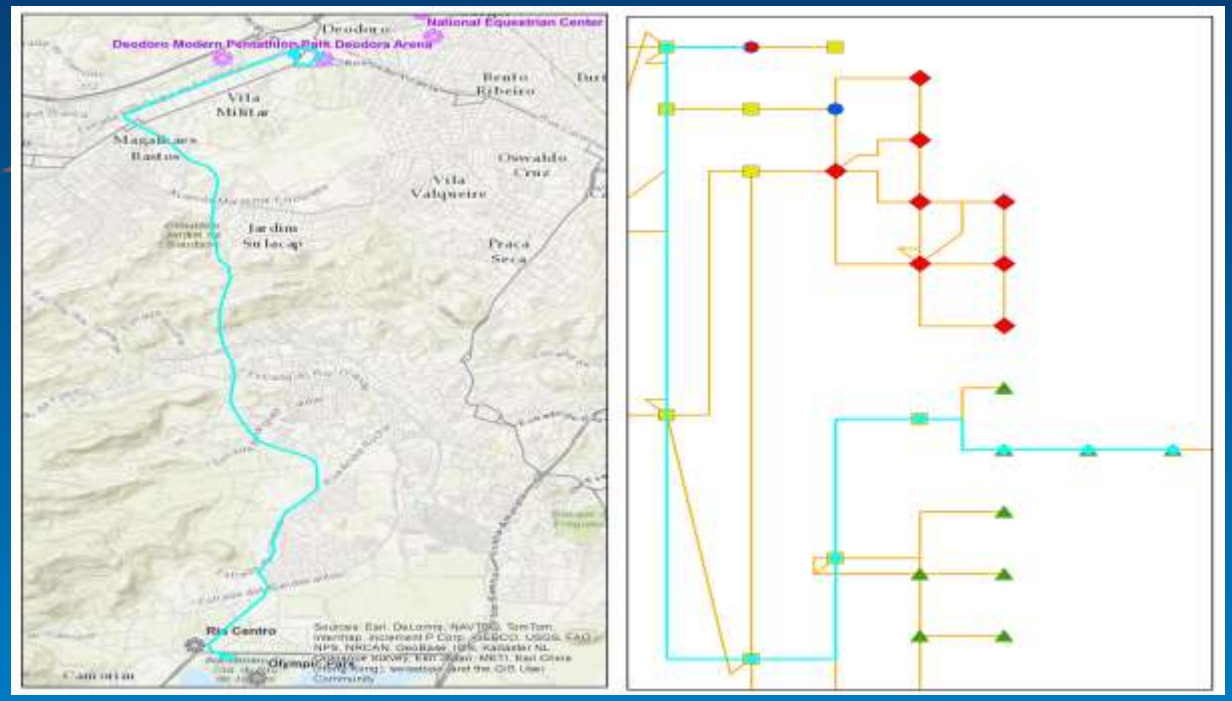
Social / Persona Layer

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

Solution Strategy

Executives / Commanders
Enterprise - focused

Operations
Process-focused

Awareness
Recovery
Prevention
Response
Protection

IT Infrastructure
Device-Focused

Cyber Security
Event-focused

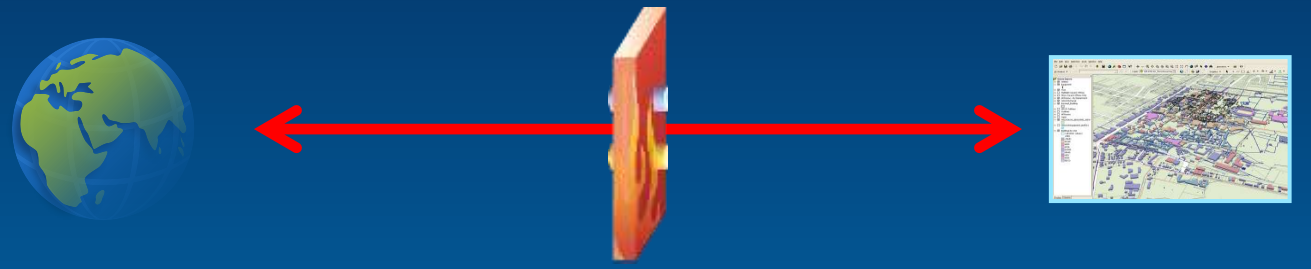
AREAS FOR IMPROVEMENT

Development of a Cyber Common Operational Picture (COP)

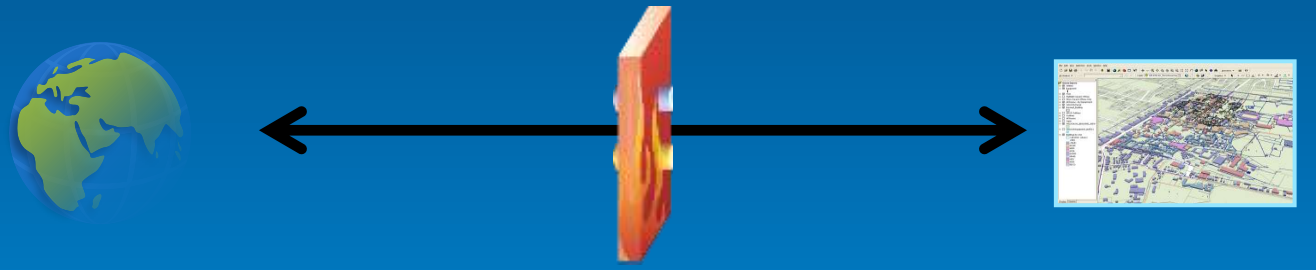
National Level Exercise 2012
Quick Look Report

Cybersecurity Activity

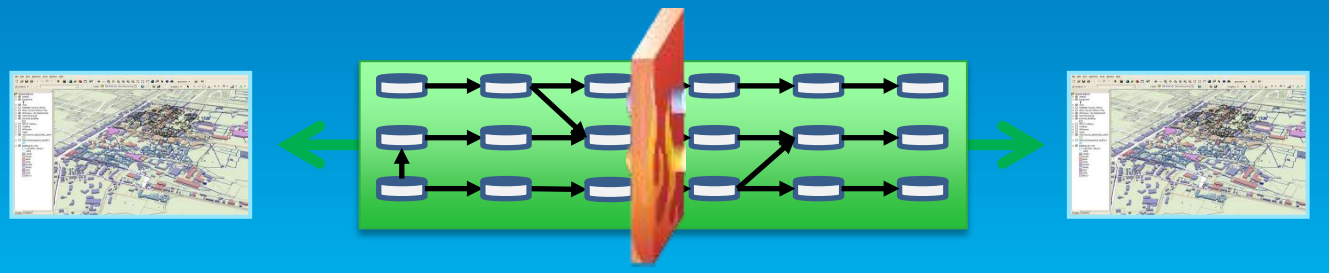
Known Bad



Anomaly Detection

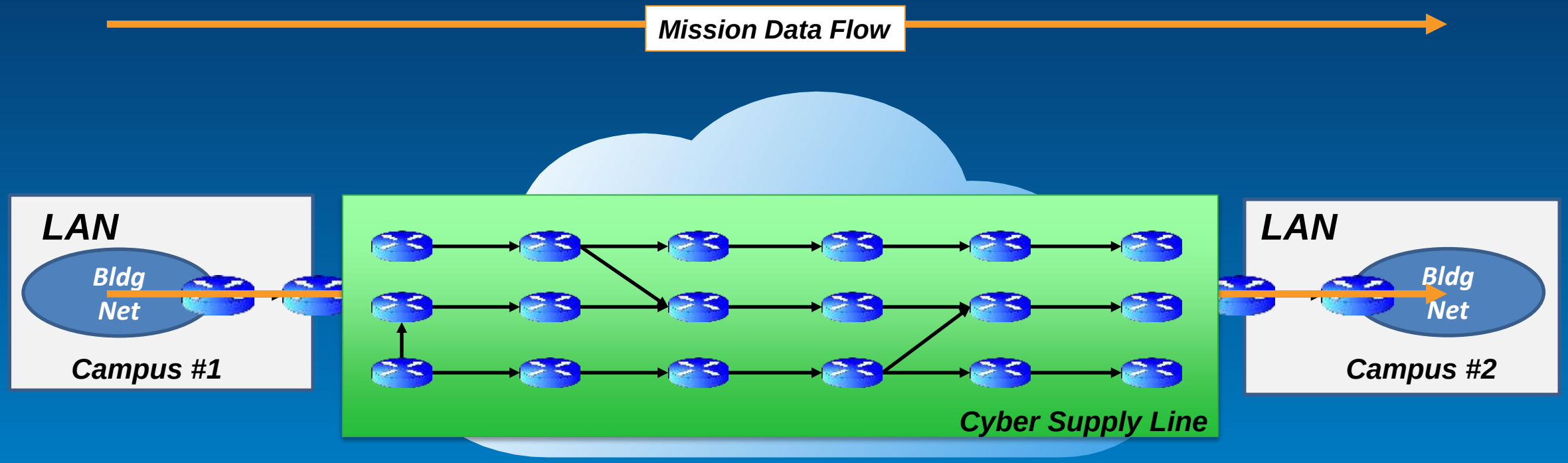


Mission Assurance
(Cyber Supply Line)



The Cyber Supply Line

A vector of devices

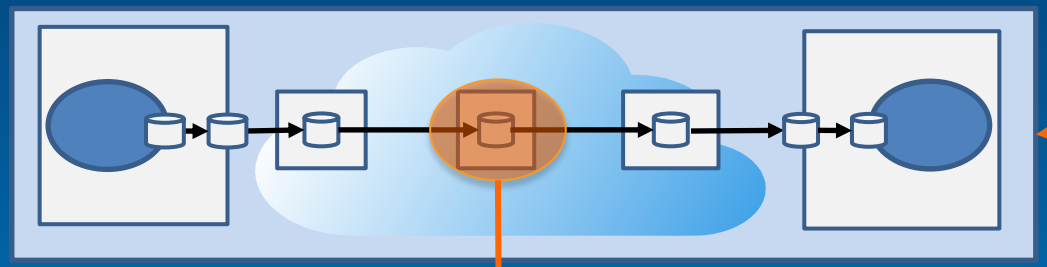


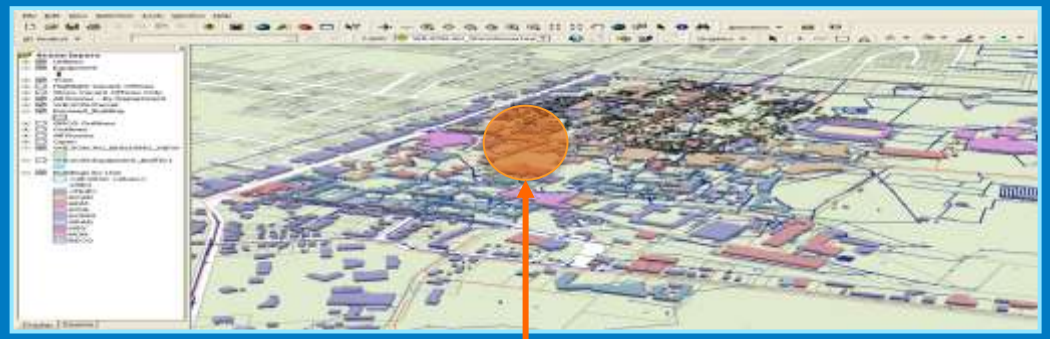
1. Cyber Supply Line (CSL) is a *consistent* path through the infrastructure
2. CSL focuses resources on only the devices that are critical
3. Managing data flows is similar to traffic routing; an Esri core competency

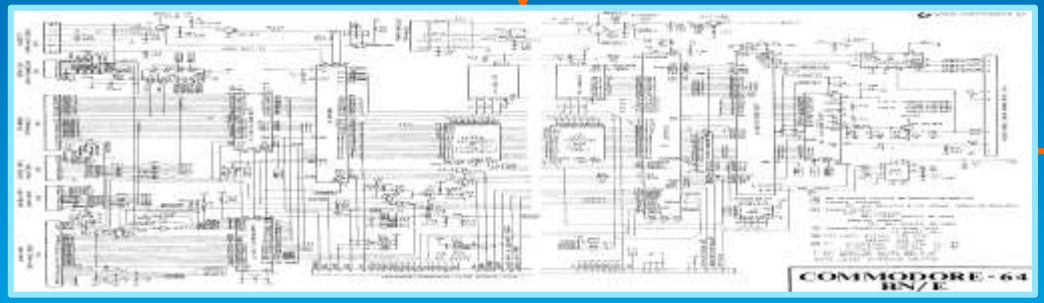
Effect Propagation

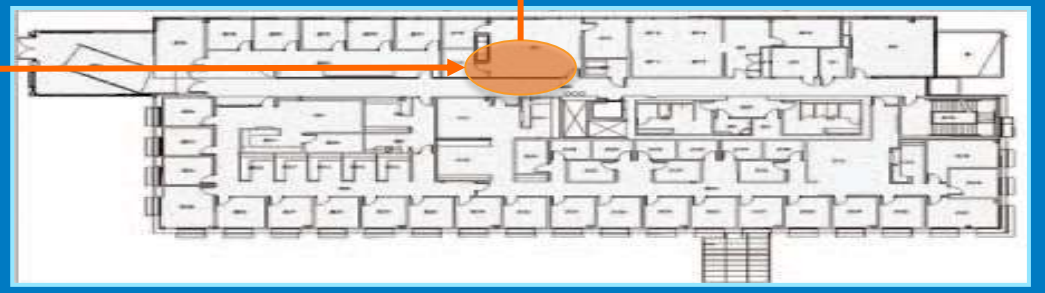
Multi-Level Model of Data Flow

Maintain Data Flow → Mission Assurance



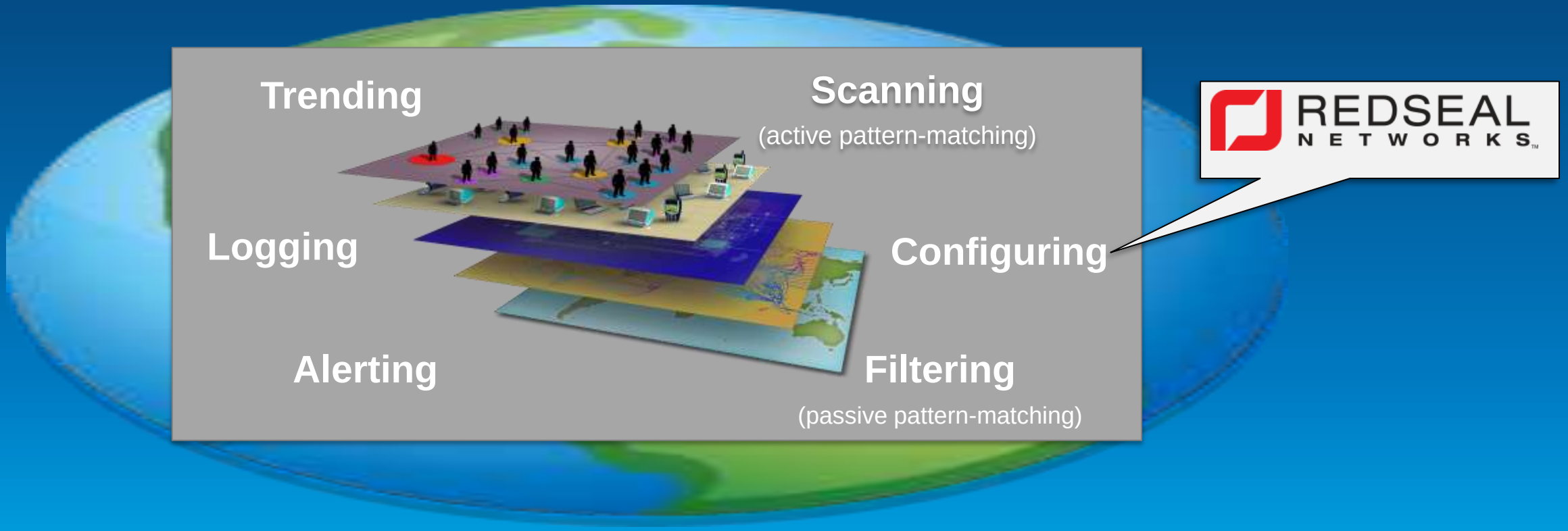






Geo-Enabling Cybersecurity

“'Geo-Enable' suggests the application of location or geospatial information as part of business processes …

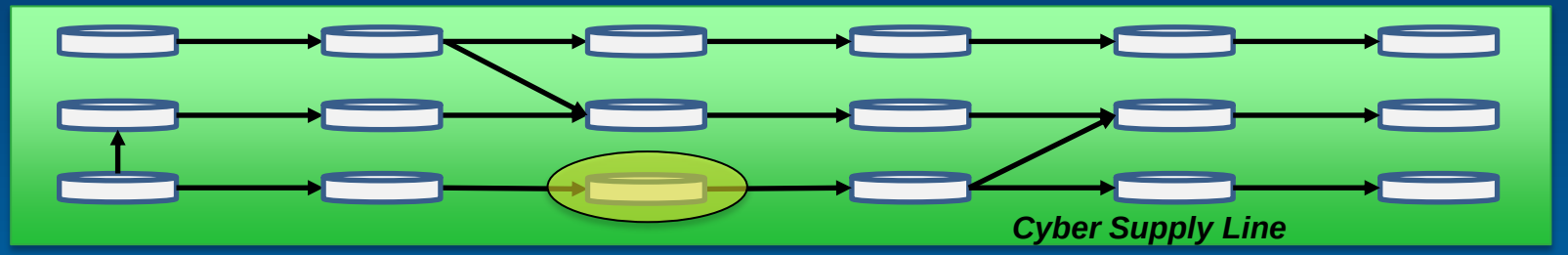


“… or using ‘location intelligence’ to augment non-spatial information systems and/or Business Intelligence (BI)”

Demonstration

Rio 2016 Olympic Games

Consolidated Cyber Framework

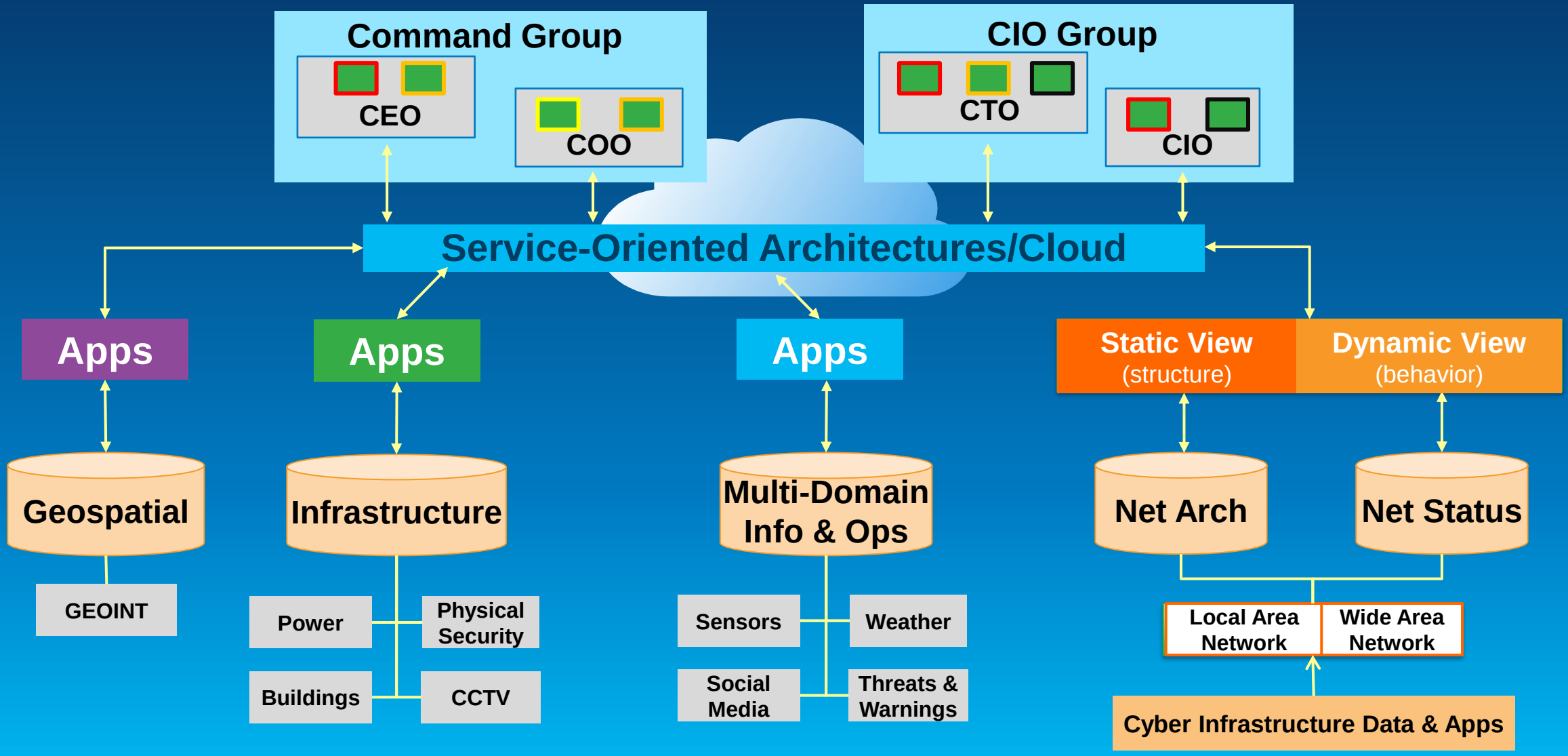


Mission Impact

	I&W		AS&W	Attack Characterization		Defense	
Target	Device Malfunction	Attack Vector	Impact Indicator	Maintenance	Attack	Mitigation	Remediation
Hardware							
Firmware							
Operating System							
Application							
Socio-Technical System							
Cyber Device (above)							
Support Devices							
Procedures							
Users							
Environment							
Social							
Physical							

Solution Strategy

Integrate Cyber into existing Operational Pictures



Implementation Outline

Source Analysis	Target Analysis (External Analysis +)	Cyber Supply Line (Target Analysis +)
ArcGIS Platform	**Facility Blueprints**	**IT Typology** (RedSeal, other)
Network Data (F/W Logs, IDS/IPS, etc.)	**IT Inventory** (device-room-function mapping)	**Mission Data Flows** (location, data, format)
Location of Sensors	**Support System Mapping** (optional)	**Other Data of Interest**
IP-to-Geolocation Service	**Other Data of Interest**	**Organizational Workflows**
Other Data of Interest	**Organizational Workflows**	
Organizational Workflows		

Cybersecurity Summary

- Geography matters for cybersecurity
- ArcGIS Platform ‘as is’ can integrate cyber with other mission data
- Multi-jurisdictional response improves mission effectiveness
- Shared Situational Awareness is more effective than direct communication

For Additional Discussion

Q&A Sessions
(The Lounge, EXPO, Hall B)

- Monday, 5:30 – 6:30
- Tuesday, 10:45 – 12:30
- Tuesday, 2:30 – 4:00

Christopher Van Dolson
Navy Cyber Defense Operations Center