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

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

- Missions / Operations
- Critical Systems
- Information Technology
- Critical Infrastructure
Solution Strategy
Integrating to improve awareness

Operations
Process-focused

Executives / Commanders
Enterprise-focused

IT Infrastructure
Device-focused

Cyber Security
Event-focused

Awareness
Recovery
Prevention
Protection
Response
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

User Defined COPs

Executive/Command
Operations

IT Group
Cyber Security

Multi-Domain Info & Ops
Social Media
Threats & Warning, Crime, 911

Weather
Sensors AVL, LPR

Geospatial
Geospatial Foundation Data

City Depts / CIKR

Ports
Transportation

Utilities
Planning

Net Status
Net Arch

Dynamic View
(behavior)
Static View
(structure)

Local Area Network
Wide Area Network

IT Organization’s Existing Data & Apps

Dashboard
Rio 2016 Olympic Games

David Attaway
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

Portal
- Desktop
- Web
- Device
- Online Content and Services
Linking your data to create the necessary relationships

<table>
<thead>
<tr>
<th>Human Resources Database</th>
<th>IT Inventory Database</th>
<th>Building</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Person</strong></td>
<td><strong>Org</strong></td>
<td><strong>Location</strong></td>
</tr>
<tr>
<td>Bill</td>
<td>Team 1</td>
<td>2Q001</td>
</tr>
<tr>
<td>John</td>
<td>Team 1</td>
<td>2Q002</td>
</tr>
<tr>
<td>Sue</td>
<td>Team 1</td>
<td>2Q003</td>
</tr>
<tr>
<td>Rick</td>
<td>Team 2</td>
<td>1W003</td>
</tr>
<tr>
<td>June</td>
<td>Team 2</td>
<td>1W004</td>
</tr>
<tr>
<td>Eva</td>
<td>Team 2</td>
<td>1W005</td>
</tr>
<tr>
<td>Dan</td>
<td>Team 2</td>
<td>1W006</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mission</th>
<th>Orgs</th>
<th>Personnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid Response Team</td>
<td>Team 1</td>
<td>Bill</td>
</tr>
<tr>
<td></td>
<td>Team 1</td>
<td>John</td>
</tr>
<tr>
<td></td>
<td>Team 1</td>
<td>Sue</td>
</tr>
</tbody>
</table>
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”