Author Request (To be completed by applicant) - The following author(s) request authority to disclose the following presentation in the MORSS Final Report, for inclusion on the MORSS CD and/or posting on the MORSS web site.

Name of Principal Author and all other author(s): Jeffrey R. Cares

Principal Author’s Organization and address:  
Alidade Incorporated  
31 Bridge Street  
Newport, RI 02840

Phone: ___401-367-0040___________  
Fax: ___401-633-6420___________  
Email: __jeff.cares@alidade.net_____

Original title on 712 A/B:  Techniques for Intelligence Analysis of Networks

Revised title:

Presented in (input and Bold one): (WG7, CG___, Special Session ___, Poster, Demo, or Tutorial):

This presentation is believed to be: 
UNCLASSIFIED AND APPROVED FOR PUBLIC RELEASE
**Techniques for Intelligence Analysis of Networks**

Alidade Incorporated


<table>
<thead>
<tr>
<th>1. REPORT DATE</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED</th>
<th>4. TITLE AND SUBTITLE</th>
<th>5a. CONTRACT NUMBER</th>
<th>5b. GRANT NUMBER</th>
<th>5c. PROGRAM ELEMENT NUMBER</th>
<th>5d. PROJECT NUMBER</th>
<th>5e. TASK NUMBER</th>
<th>5f. WORK UNIT NUMBER</th>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
<th>10. SPONSOR/MONITOR’S ACRONYM(S)</th>
<th>11. SPONSOR/MONITOR’S REPORT NUMBER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 JUN 2005</td>
<td>N/A</td>
<td>-</td>
<td>Techniques for Intelligence Analysis of Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES


14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

17. LIMITATION OF ABSTRACT

UU

18. NUMBER OF PAGES

12

19a. NAME OF RESPONSIBLE PERSON

unclassified

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
Techniques for Intelligence Analysis of Networks

Jeffrey R. Cares

73rd MORSS

©2005 Alidade Incorporated. All Rights Reserved
Main Points

• “Complex Networks” have exploitable properties
  – e.g.: Information Age commercial/social successes
• These exploitable properties have military relevance
  – e.g.: Sense and Respond Logistics (OSD-FT)
• There are significant intelligence analysis manifestations of these properties
• A more satisfying theory of Networked Competition (than currently exists for NCW/NCO, etc) is emerging from this research
## Network Metric Thumb Rules
### Experimentation and Analysis

<table>
<thead>
<tr>
<th>Metric</th>
<th>Range</th>
<th>Operational Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes, $n$</td>
<td>$n &gt; \sim 100$</td>
<td>Network effects unlikely to occur with $n &lt; 50$</td>
</tr>
<tr>
<td>Number of links, $l$</td>
<td>$l &lt; \sim 2n$</td>
<td>$l &lt; &lt; 2n$, too brittle</td>
</tr>
<tr>
<td></td>
<td>$l &gt; &gt; 2n$, too much overhead</td>
<td></td>
</tr>
<tr>
<td>Degree distribution</td>
<td>Skewed</td>
<td>Adaptivity, modularity</td>
</tr>
<tr>
<td>Largest hub</td>
<td>&lt; 100 links</td>
<td>Hub appears, recedes by reconnection 5% of links</td>
</tr>
<tr>
<td>Average path length</td>
<td>$\log(n)$</td>
<td>Short distances even for large networks (e.g., $10^4$ nodes $\Rightarrow$ Average path length $\sim 4$)</td>
</tr>
<tr>
<td>Clustering</td>
<td>Skewed</td>
<td>Hierarchy, organization</td>
</tr>
<tr>
<td>Betweenness</td>
<td>Skewed</td>
<td>Cascade control</td>
</tr>
<tr>
<td>Path horizon</td>
<td>$\log(n)$</td>
<td>Self-synchronization</td>
</tr>
<tr>
<td>Susceptibility/Robustness</td>
<td>Low (random removal)</td>
<td>Hubs should be kept obscure until needed, damage abatement/repair schemes</td>
</tr>
<tr>
<td></td>
<td>High (focused removal)</td>
<td></td>
</tr>
<tr>
<td>Neutrality Rating</td>
<td>$(0, 1)$</td>
<td>Increased network effects, decreased susceptibility, tipping points</td>
</tr>
<tr>
<td>Coefficient of Networked Effects</td>
<td>$(0, 1)$</td>
<td>Network effects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PFE/$n$</td>
</tr>
</tbody>
</table>
Number of Nodes, Links

- A factor in how many links are required for adaptive behavior
  - A very large number of nodes with low link density suggests a brute force strategy
  - A very large number of nodes with high link density suggests confusion
  - A very small number of nodes with high link density suggests tight-knit cabal
  - A very small number of nodes with low link density suggests a brittle organization

- Potential Strategy
  - Drive the link/node ratio in a direction counter to what the target organization may need for assumed mission
Degree Distribution

- **Skewed: Adaptive, Learning Organization**
  - Hubs can be kept obscure until needed
  - Hubs can recede, re-appear with re-wiring of 5-10% of links
  - All paths to hubs are short

- **Uniform (Lattice): Strict Hierarchy**
  - As average degree tends toward 1 organization becomes more “chain-like” and brittle

- **Multi-modal: Dispersed Operations**

- **Potential Strategies**
  - Skewed: encourage hub formation, follow short paths
  - Uniform: reduce average degree (increase brittleness)
  - Multi-modal: Divide and conquer
Clustering

- High: Small World Effect
- Low: Strict Hierarchy
- Skewed: Adaptive
- Potential Strategies
  - High: Follow short paths to target nodes
  - Low: Drive toward brittleness
  - Skewed: Look for “President’s Cluster”
Betweenness

- Nodes with high betweenness are nodes through which the highest number of shortest paths pass

- Potential Strategies
  - Bombard the target network with noise to flush out high betweenness
  - Keep high betweenness nodes alive until the target network needs them most
  - Look at low degree nodes close to high betweenness for gatekeeper-protected node relationships
Path Horizon

- Very Low: Tight coordination
- \( \log(n) \): Adaptive
- High: Chains
- Potential Strategies
  - Very Low: Bombard with noise
  - \( \log(n) \): Induce different structure on network
  - High: Interdict
CNE ($h$-cycles)

- Low $h$: Tight coordination
- High $h$: Chain
- Potential Strategy:
  - Low $h$: bombard with noise
  - High $h$: Remove links to turn into low $h$ and then bombard with noise
Conclusions

• Structural Analysis is a useful tool for understanding networks
• Strong complement to traditional methods
• Provides recommendations for how to attack or influence the target network
• Most examples are from non-military contexts
  – Need for military-specific research
Questions?