Visual Analytics for cyber security and intelligence
Valerie Lavigne and Denis Gouin

Presented by Hancheng Zhao

CISC850
Cyber Analytics
1. Introduction

• Needs: identify trends and patterns promptly.

• Visual Analytics (VA): representing the information and providing mechanisms to interact with

• Main content: a quick overview of the current state of the art in VA and its future
2. Visual Analytics

• “Visual analytics is the science of analytical reasoning facilitated by interactive visual interfaces.” -- US research Agenda

• A multidisciplinary field
2.1 Visualization

• should be designed in a meaningful way in order to provide insight to the user.

• Pre-attentive visual features:
2.2 Interaction

• 3 categories of responsiveness:
  – 0.1s: upper limit to feel instantaneous
  – 1s: lose feeling of operating directly on the data
  – 10s: want to perform other tasks while waiting

• mantra: “overview first, zoom/filter, details on demand””
2.3 Analytical reasoning

3 goals:
- **assessment** (understand current situation and explain past events)
- **forecasting** (estimate future capabilities and threats)
- **planning** (prepare reactions to potential events)
3. Advanced VA concepts and techniques

- NodeTrix social network visualization.
  - adjacency matrices
  - useful in globally sparse but locally dense social networks
3. Advanced VA concepts and techniques

• Treemap: markets on November 23, 2010.
  – used to spot trends and investment opportunities.
3. Advanced VA concepts and techniques

- Parallel coordinates

Extended parallel coordinates view representing car attributes.
3. Advanced VA concepts and techniques

• Dust & Magnets metaphor

Dust & Magnet example using a cereal dataset.
3. Advanced VA concepts and techniques

- VisLink:
4. Cyber security

- VA can improve cyber security with capabilities to:
  - recognize risks and protect against cyber threats
  - enable key aspects of the digital forensic process
  - allow information discovery, processing and visualization.
4. Cyber security

Relationship between the stages of situational awareness, the uses of visualization and the types of analysis performed.
4. Cyber security

- The NFlowVis Network visualization: large-scale network traffic monitoring and distributed attacks detecting.
4. Cyber security

- The NFlowVis Network visualization: large-scale network traffic monitoring and distributed attacks detecting.

Example of NFlowVis showing communication flows between source and destination hosts.
4. Cyber security

- ManyNets is a tool for the simultaneous visualization of many networks.
4. Cyber security

- History trees
4. Cyber security

- Visualization that shows nearly 34,000 vulnerabilities identified by three software analysis tools.
5. Intelligence, counterterrorism and counter-insurgency

Design implications for systems supporting intelligence analysis:

- externalize the thinking process

- support source management

- support analysis with constantly changing information

- help analysts create convincing production

- unifying the pieces
5. Intelligence, counterterrorism and counter-insurgency

The IN-SPIRE discovery tool
5. Intelligence, counterterrorism and counter-insurgency

Theme River representation of terrorism attacks in the world over time.
5. Intelligence, counterterrorism and counter-insurgency

Analysis of Improvised Explosive Devices in Iraq with BOOMsys.
5. Intelligence, counterterrorism and counter-insurgency

Oculus GeoTime interface.

- Time-space annotations of events
### 6. Moving forward

**Table 2. Evaluation approaches.**

<table>
<thead>
<tr>
<th>Method</th>
<th>Most useful for...</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observations and interviews</td>
<td>Revealing analytic process</td>
<td>Subjective</td>
</tr>
<tr>
<td>Questionnaires and discussion groups</td>
<td>Usability testing – user satisfaction with system</td>
<td>May not reflect true utility/effectiveness</td>
</tr>
<tr>
<td>Heuristic evaluation</td>
<td>Usability testing – focus on user interactions/transactions with system</td>
<td>May not reveal deeper insights of cognitive process</td>
</tr>
<tr>
<td>Longitudinal studies</td>
<td>In-depth assessment of extent to which tool aligns with process</td>
<td>Tends to use a small sample of participants</td>
</tr>
<tr>
<td>Controlled experiments/performance testing</td>
<td>Comparing alternative VA approaches leading to enduring scientific conclusions</td>
<td>Difficulty in obtaining sufficient number of participants</td>
</tr>
</tbody>
</table>

VA: Visual Analytics.
7. Conclusion

- VA has emerged as a significant multidisciplinary research field that leverages the human cognitive abilities

- VA is making its way into defense and security applications, such as cyberspace management and intelligence analysis

- VA has a significant momentum and VA research and applications have been growing exponentially over recent years