CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Visual Analytics for Decision Making

VACCINE (CVADA)

Kaethe Beck

Sept. 17 2013

Homeland Security

Science and Technology

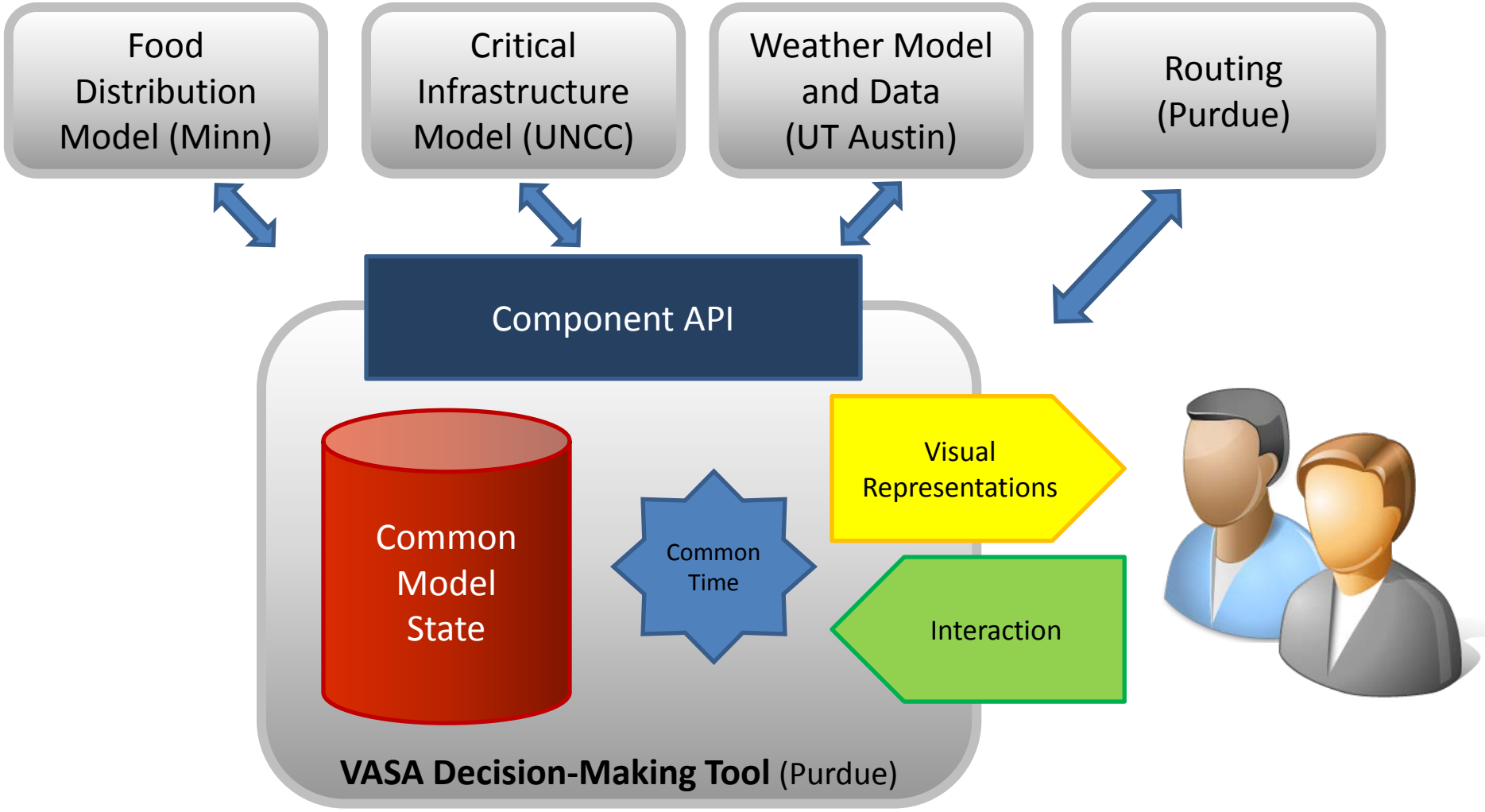
Team Profile

- Who We Are: Team of International Experts
  - 25 Institutions, 75+ Faculty
- What We Do: Help individuals find relevant, useful information from big data to aid in rapid, accurate decision making
- Who We Work With: USCIS, CBP, 40+ Law Enforcement Agencies and First Responder Groups, USCG, TSA, US CERT, US Federal Emergency Management Agency, Fusion Centers

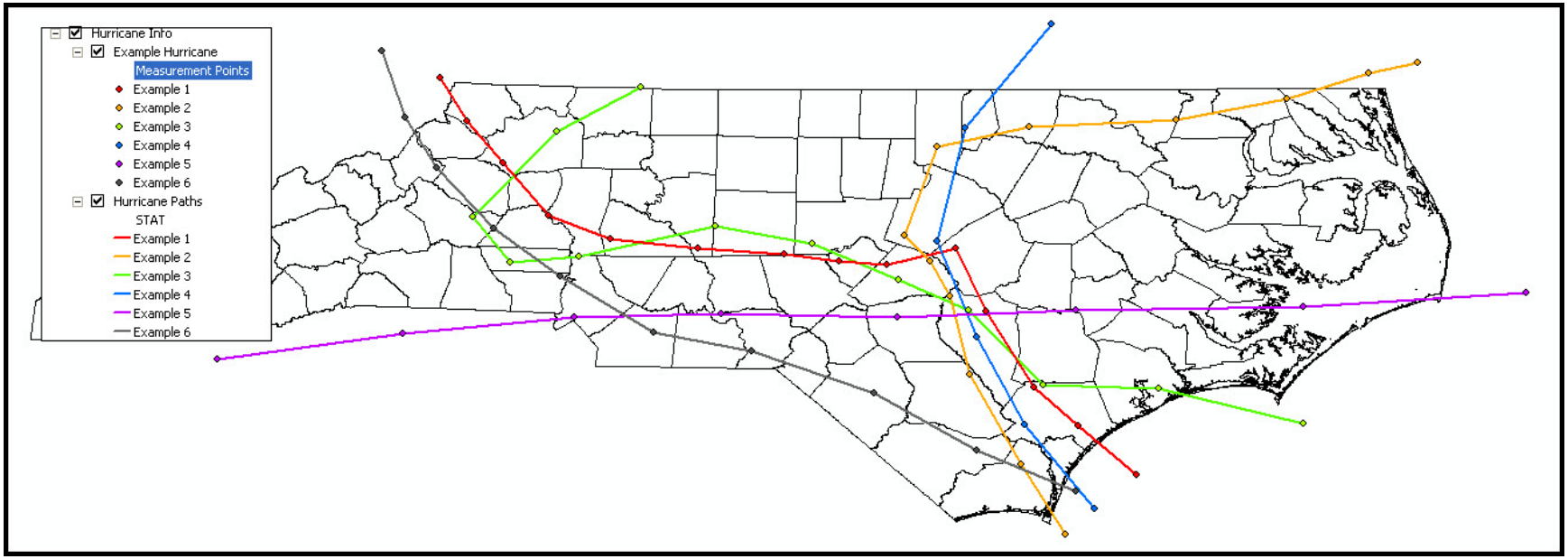
VACCINE Projects

- VASA
- Sensor Forensics
- Corporate Insider Threat Detection
- SemanticPrism
- Scatterblogs
- Jigsaw
- Spring Rain*

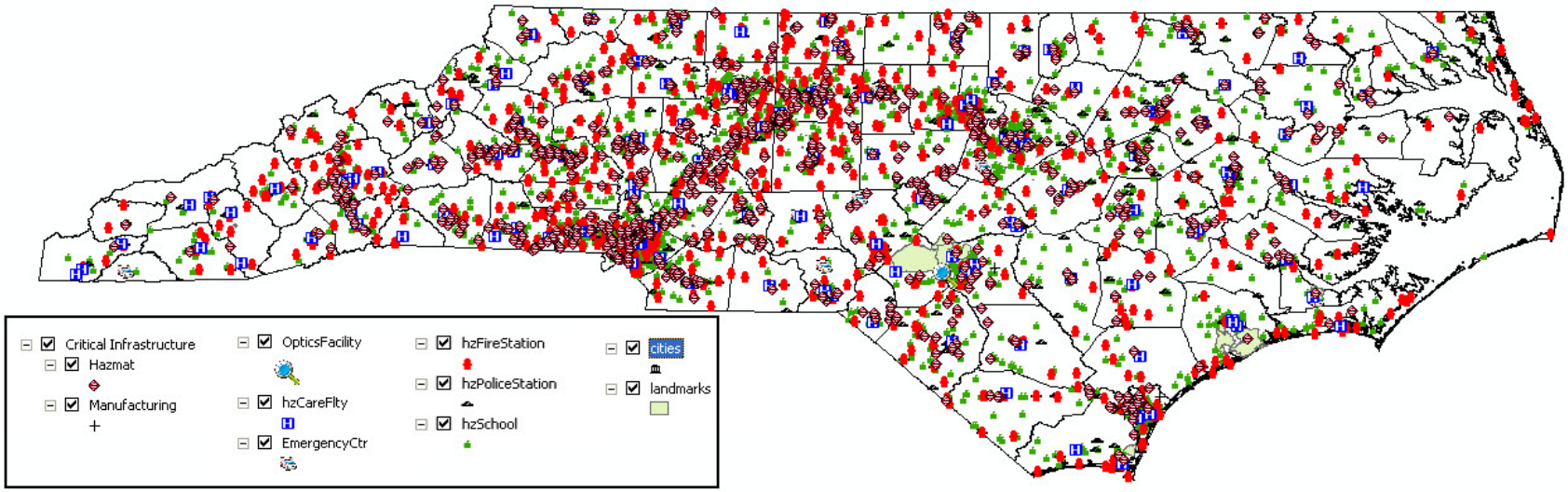
VASA


Food Distribution Model (Minn)
Critical Infrastructure Model (UNCC)
Weather Model and Data (UT Austin)
Routing (Purdue)
Component API
Common Model State
Common Time
Visual Representations
Interaction
VASA Decision-Making Tool (Purdue)

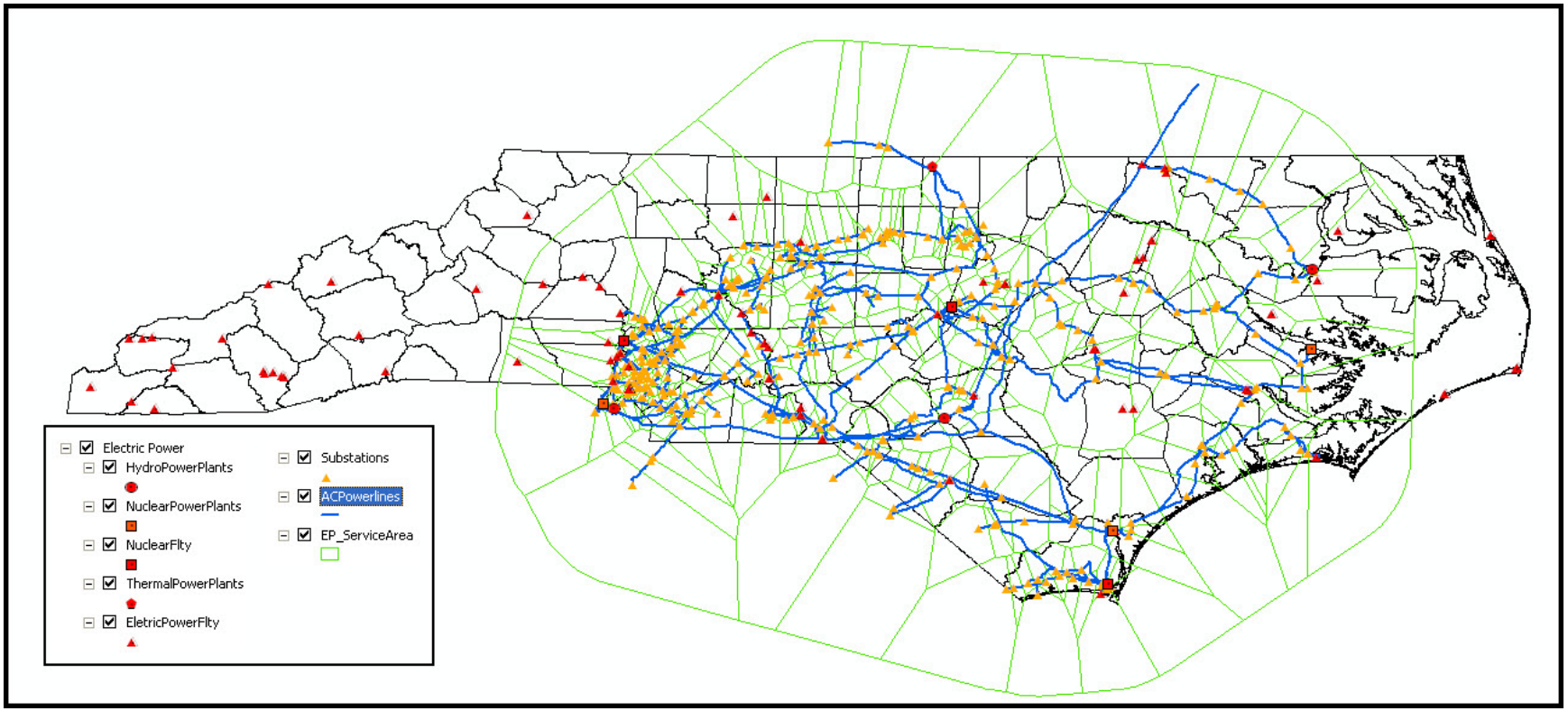
VASA


Hurricane Info
Example Hurricane
Measurement Points
Example 1
Example 2
Example 3
Example 4
Example 5
Example 6
Hurricane Paths
STAT
Example 1
Example 2
Example 3
Example 4
Example 5
Example 6

VASA


Critical Infrastructure
Hazmat
Manufacturing
OpticsFacility
hzCareFlty
EmergencyCtr
hzFireStation
hzPoliceStation
hzSchool
cities
landmarks

VASA


Electric Power
HydroPowerPlants
NuclearPowerPlants
NuclearFlty
ThermalPowerPlants
EletricPowerFlty
Substations
ACPowerlines
EP_ServiceArea

Sensor Forensics

- Forensic characterization
  - Observe device output ➔ which device produced it?
  - Exploit how the device “makes” its output
- Device authentication
  - Performed using forensic characterization
  - Identify device type, make, model, configuration
  - Can the sensor be trusted?
- Detection of data forgery or alteration
- Fingerprint and trace

Corporate Insider Threat Detection

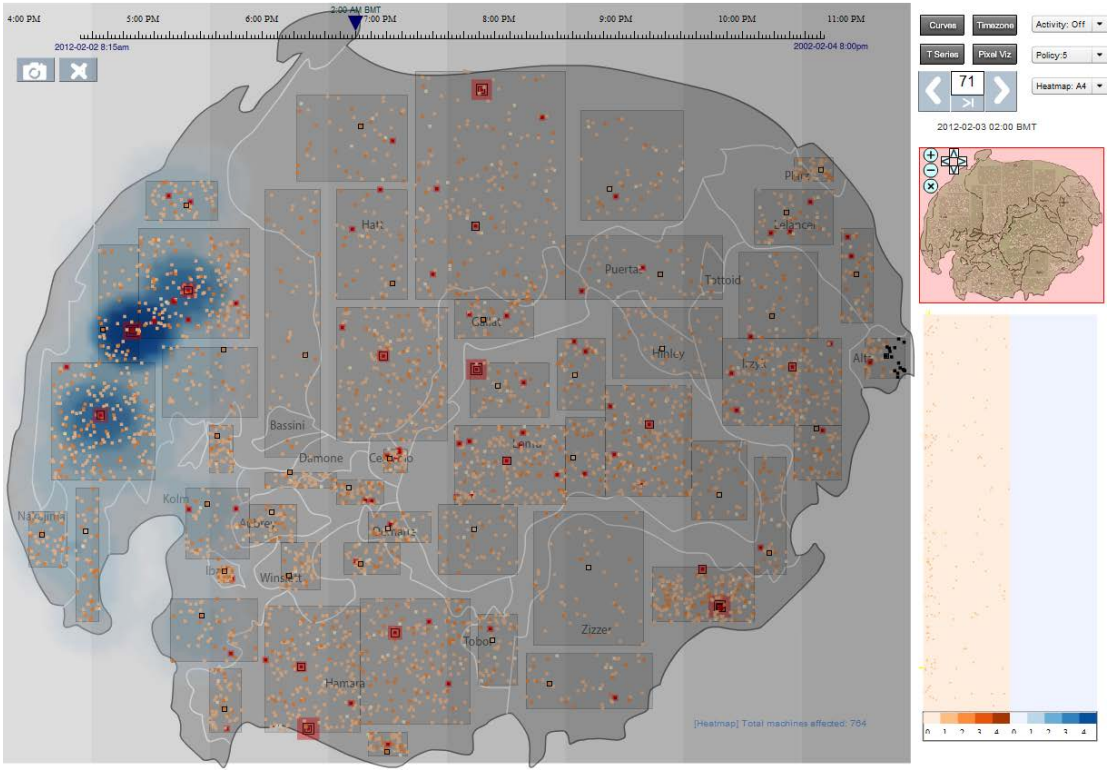
- **Sponsor:** Centre for the Protection of National Infrastructure
- **Academics:** Sadie Creese (PI), Min Chen, Michael Goldsmith, Michael Levi, David Upton and Monica Whitty
- **Combined Expertise** in cyber security, psychology, criminology, visual analytics, enterprise operations management and executive education
- **Objectives:**
  - Develop a model,
  - Understand psychological indicators
  - Identify the most effective algorithms
  - Understand enterprise culture and common practices
  - Provide a **visual analytical** interface
  - Develop an understanding of both the various organisational roles and awareness raising and educational methods
- **URL:** http://www.cs.ox.ac.uk/projects/CITD/index.html
- **Oxford Cybersecurity Centre:** http://www.cybersecurity.ox.ac.uk/index.html

SemanticPrism: A Multi-aspect View of Large High-dimensional Data

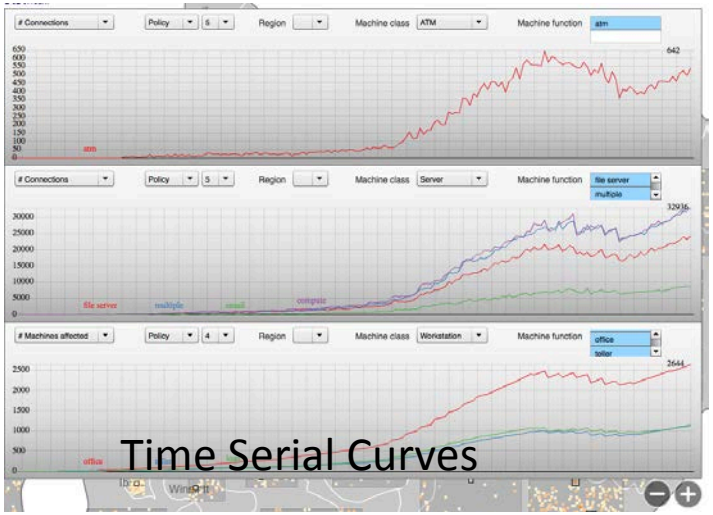
- VAST 2012 Mini Challenge 1 Award:
  Outstanding Integrated Analysis and Visualization

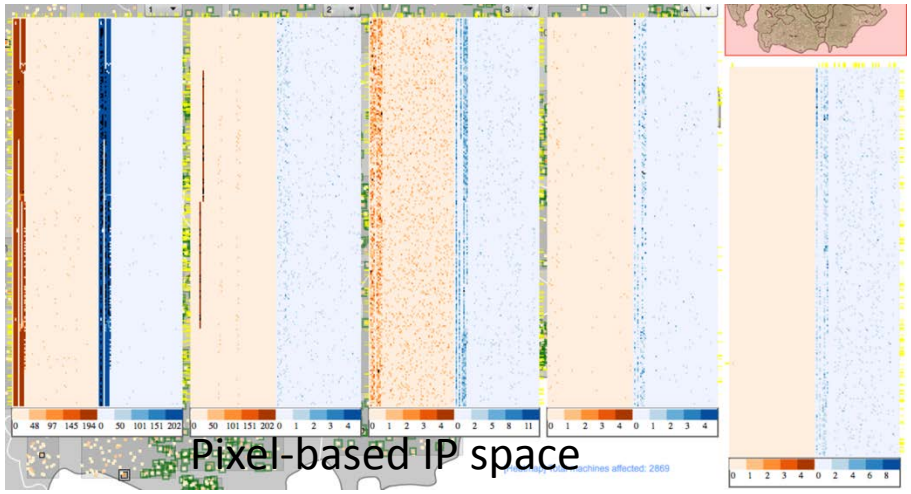
- Geo-Temporal
- Time-serial
- Pixel-based

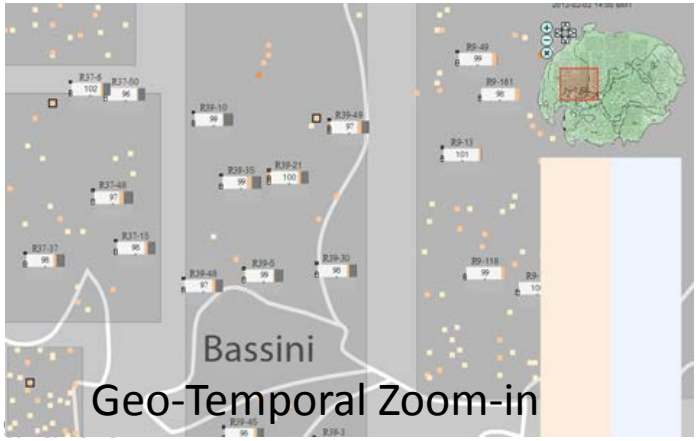
- Semantic Zoom

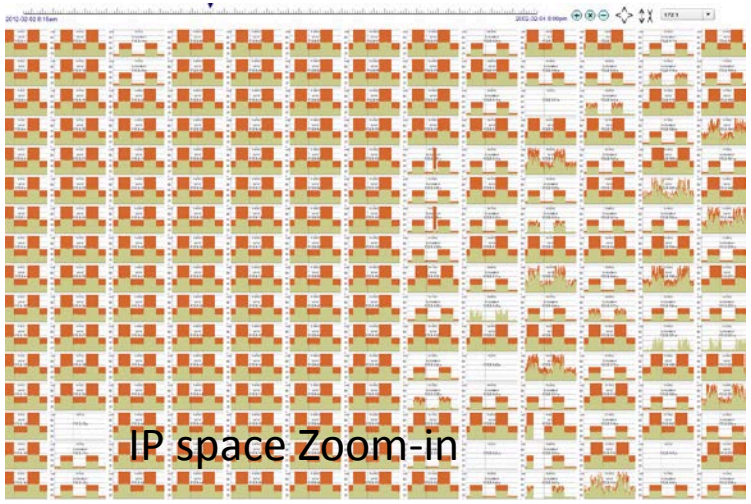


SemanticPrism

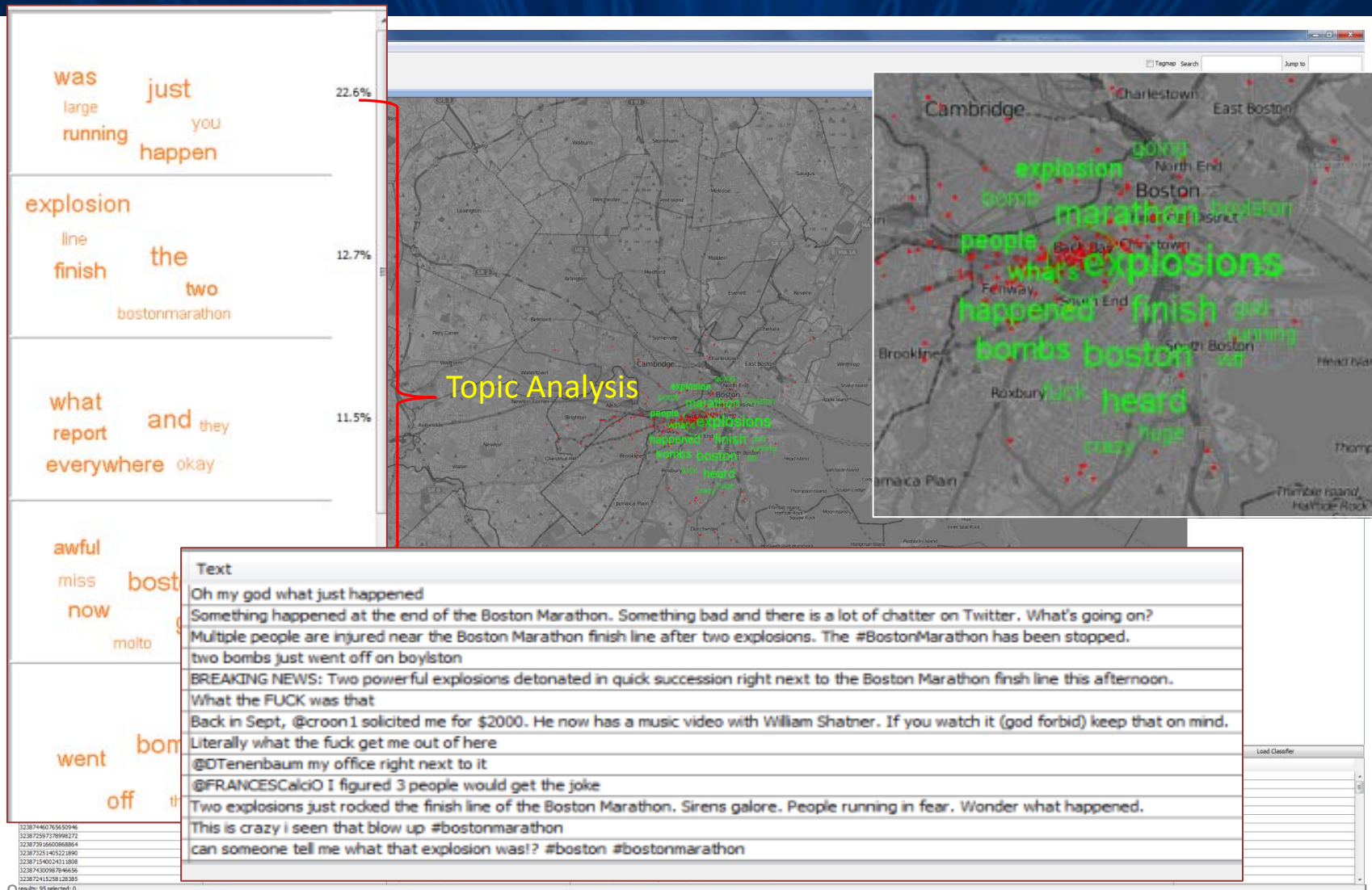






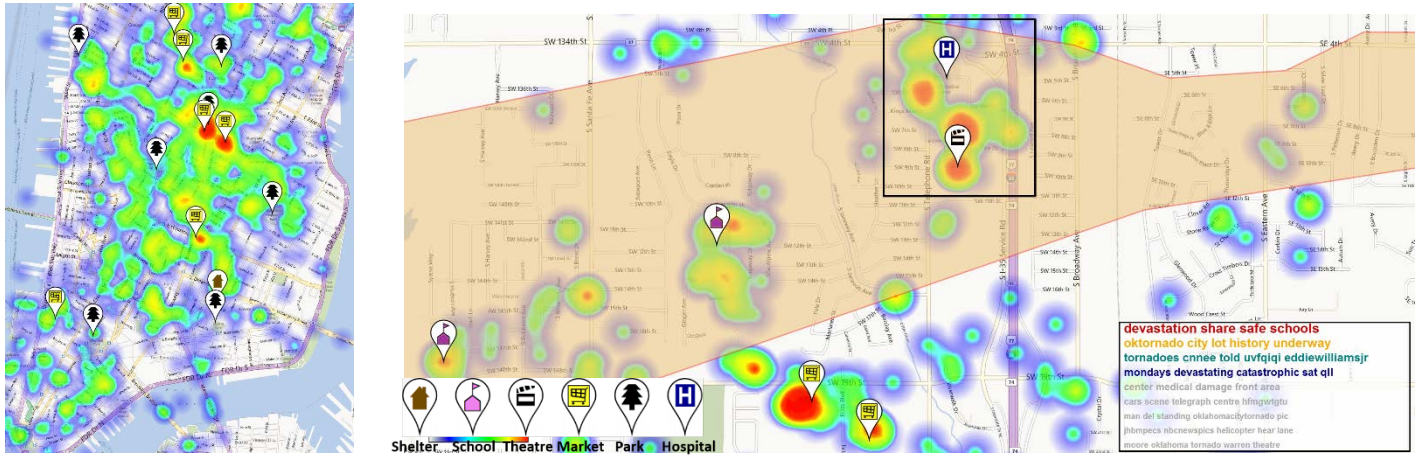


Scatterblog



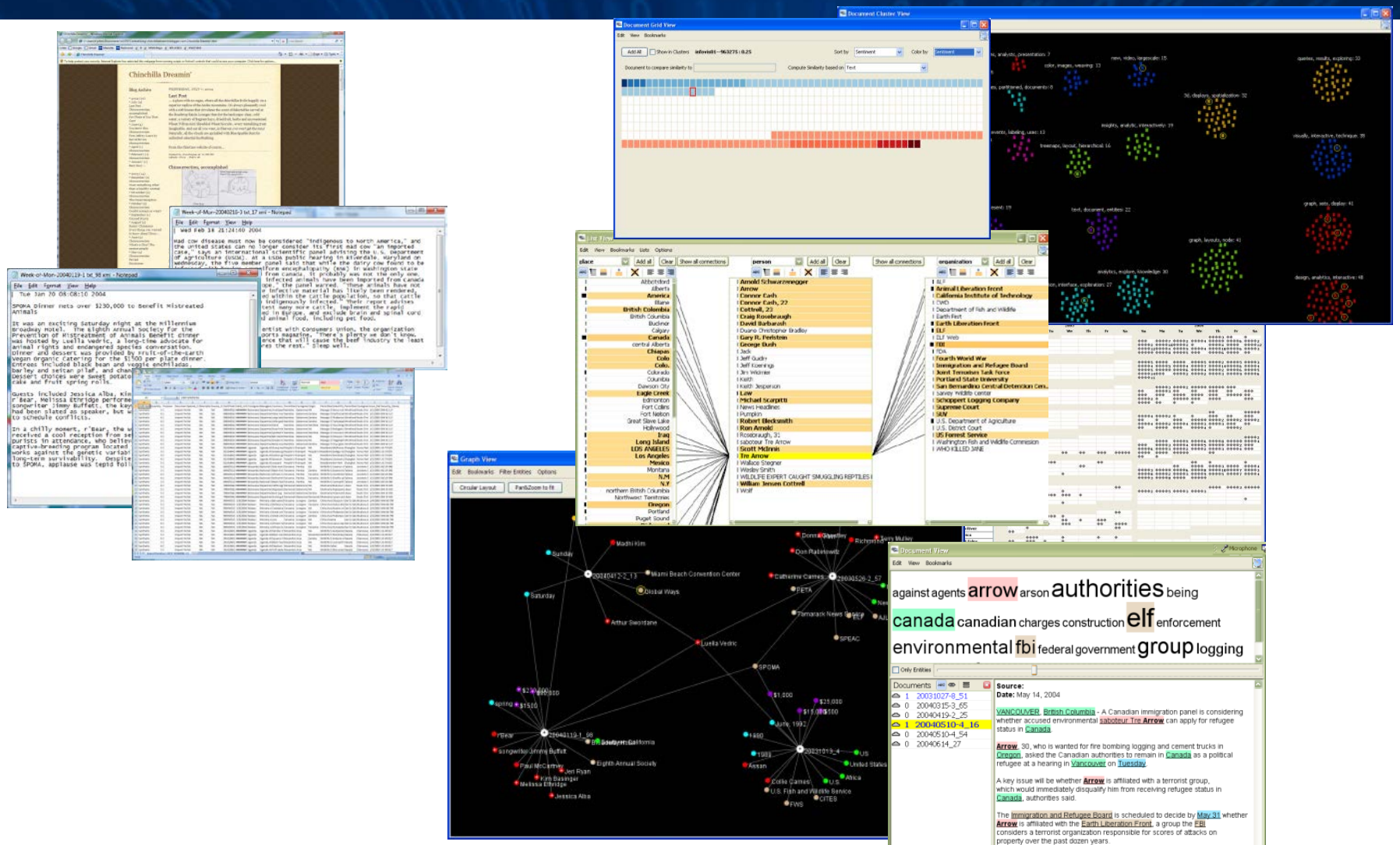
Scatterblog

- Location-based Social Network data has substantial potential to increase situational awareness.

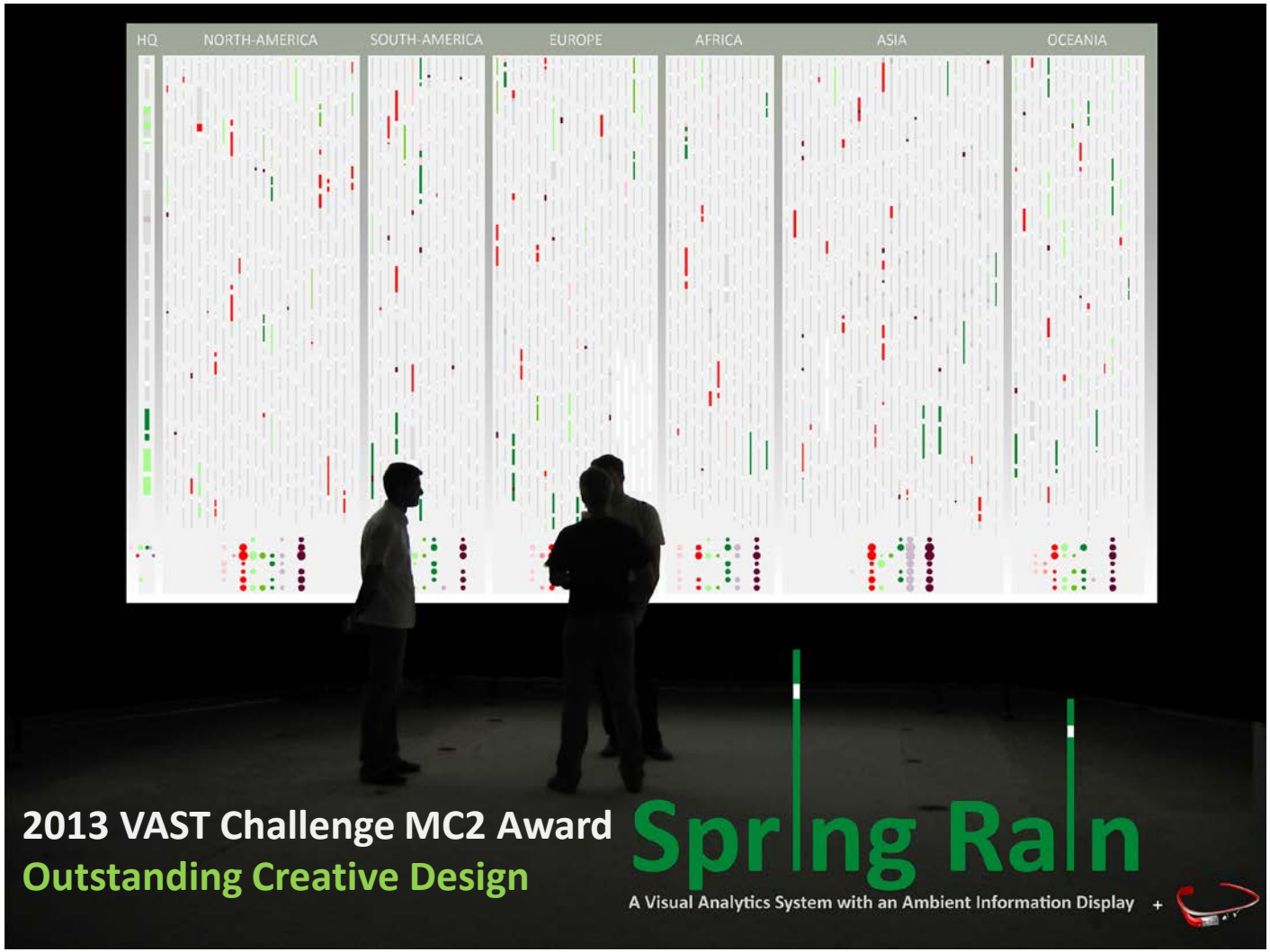


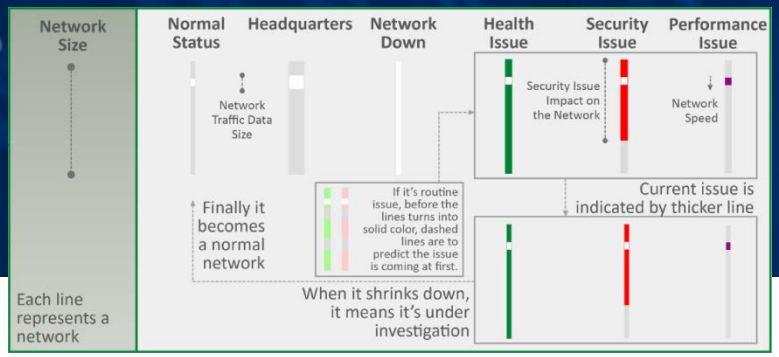
Spatial user-based Tweet distribution during four hours right after evacuation order for Hurricane Sandy on October 28th, 2013 (Left). A relatively large number of people immediately went to super markets nearby the evacuation area, instead of the emergency shelter. Spatial pattern of Twitter users during 24 hours in the city of Moore after damages from a strong tornado (Right). Relatively many people moved to severely damaged areas after the disaster. Topic cloud (Right-Bottom): Topics from Tweets within the selected area with a box. The topics are ordered by their abnormality scores

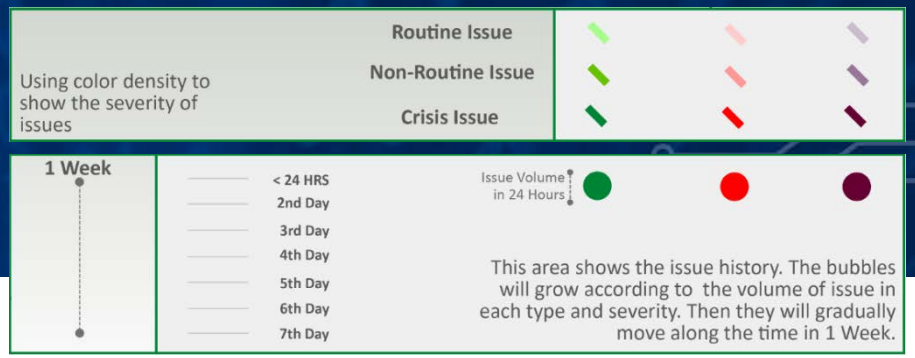
Jigsaw: Visual Analytics for Investigative Analysis

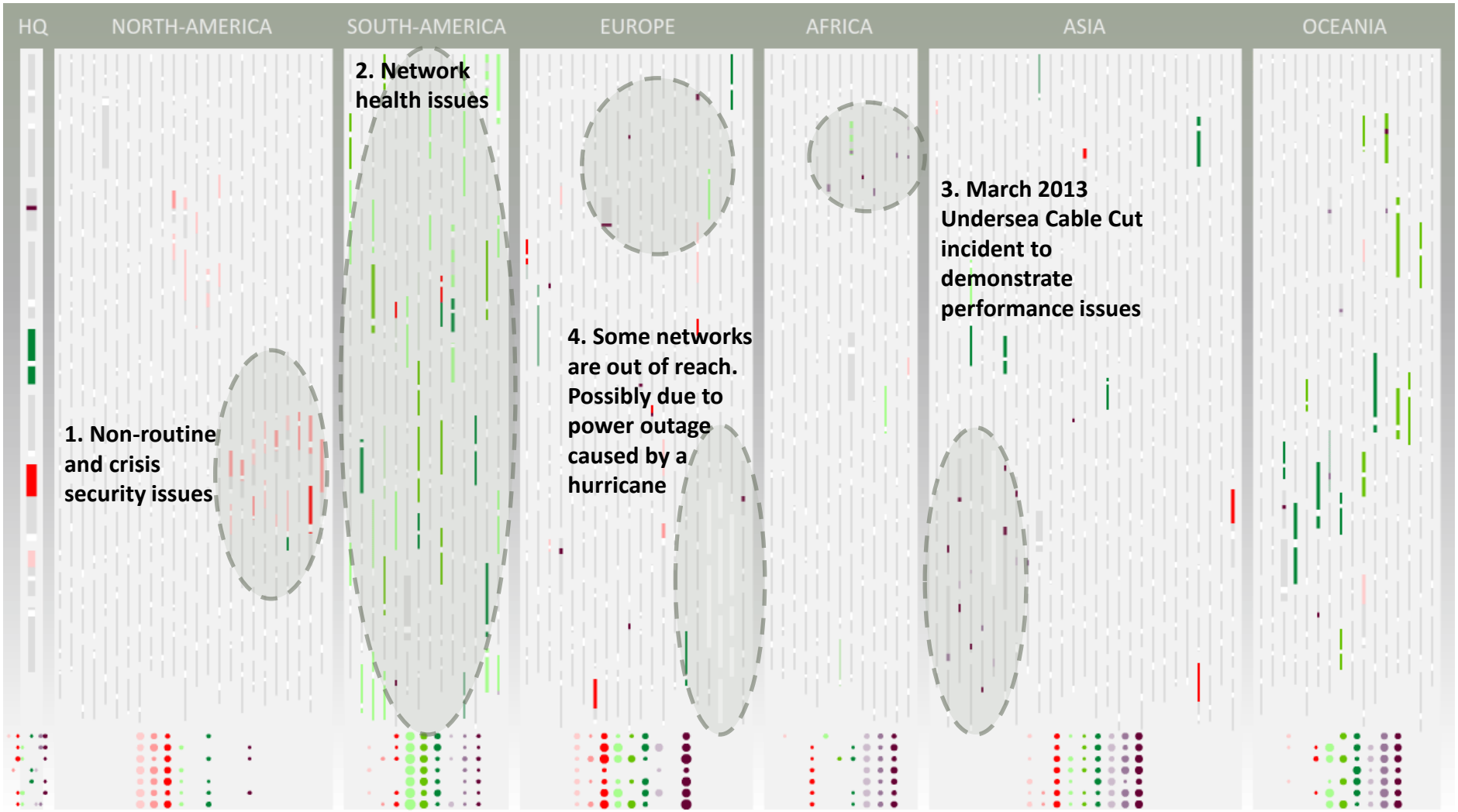


Spring Rain


HQ
NORTH-AMERICA
SOUTH-AMERICA
EUROPE
AFRICA
ASIA
OCEANIA
2013 VAST Challenge MC2 Award
Outstanding Creative Design
Spring Rain
A Visual Analytics System with an Ambient Information Display +


Network Size
Each line represents a network
Normal Status
Headquarters
Network Down
Health Issue
Security Issue
Performance Issue
Network Traffic Data Size
Security Issue Impact on the Network
Network Speed
Finally it becomes a normal network
If it's routine issue, before the lines turns into solid color, dashed lines are to predict the issue is coming at first.
Current issue is indicated by thicker line
When it shrinks down, it means it's under investigation


Using color density to show the severity of issues
Routine Issue
Non-Routine Issue
Crisis Issue
1 Week
< 24 HRS
2nd Day
3rd Day
4th Day
5th Day
6th Day
7th Day
Issue Volume in 24 Hours
This area shows the issue history. The bubbles will grow according to the volume of issue in each type and severity. Then they will gradually move along the time in 1 Week.


HQ
NORTH-AMERICA
SOUTH-AMERICA
EUROPE
AFRICA
ASIA
OCEANIA
1. Non-routine and crisis security issues
2. Network health issues
3. March 2013 Undersea Cable Cut incident to demonstrate performance issues
4. Some networks are out of reach. Possibly due to power outage caused by a hurricane

Contact Information

- Kaethe Beck – kaethe@purdue.edu

www.VisualAnalytics-CCI.org

Financial Risk