Designing STAR: A Cyber Dashboard Prototype

Sean McKenna, University of Utah & MIT Lincoln Laboratory

Problem: Communication of Cyber Information

- **Why?**
  - Technical jargon
  - Lack (or bloat) of tools
  - Manual work to convey information
  - Quantity and time-scale of data
  - Impact and effects on daily operations

Personas

CEO (decision-making)

Goals	Coordinate personnel and operations	
Knowledge	Operations ●●●●●	Cyber ●○○○○
Cyber SA	Attention ●○○○○	Temporal Window ◄——►
Key Questions	• How can we maintain ongoing operations? • What could happen if a critical system is impacted? • What are the most critical systems at risk of attack? • What cyber resources will be needed in the future?	

Decisions

Director of IT (decision-making)

Goals	Maintain cyber situational awareness	
Knowledge	Operations ●●●○○	Cyber ●●●○○
Cyber SA	Attention ●●○○○	Temporal Window ◄——►
Key Questions	• Does this attack matter? • How serious is the attack? • What do I do about the attack? • Are there any negative effects?	• What did the bad guys do/take? • Is it a good day on the network? • How is my network different from last week?

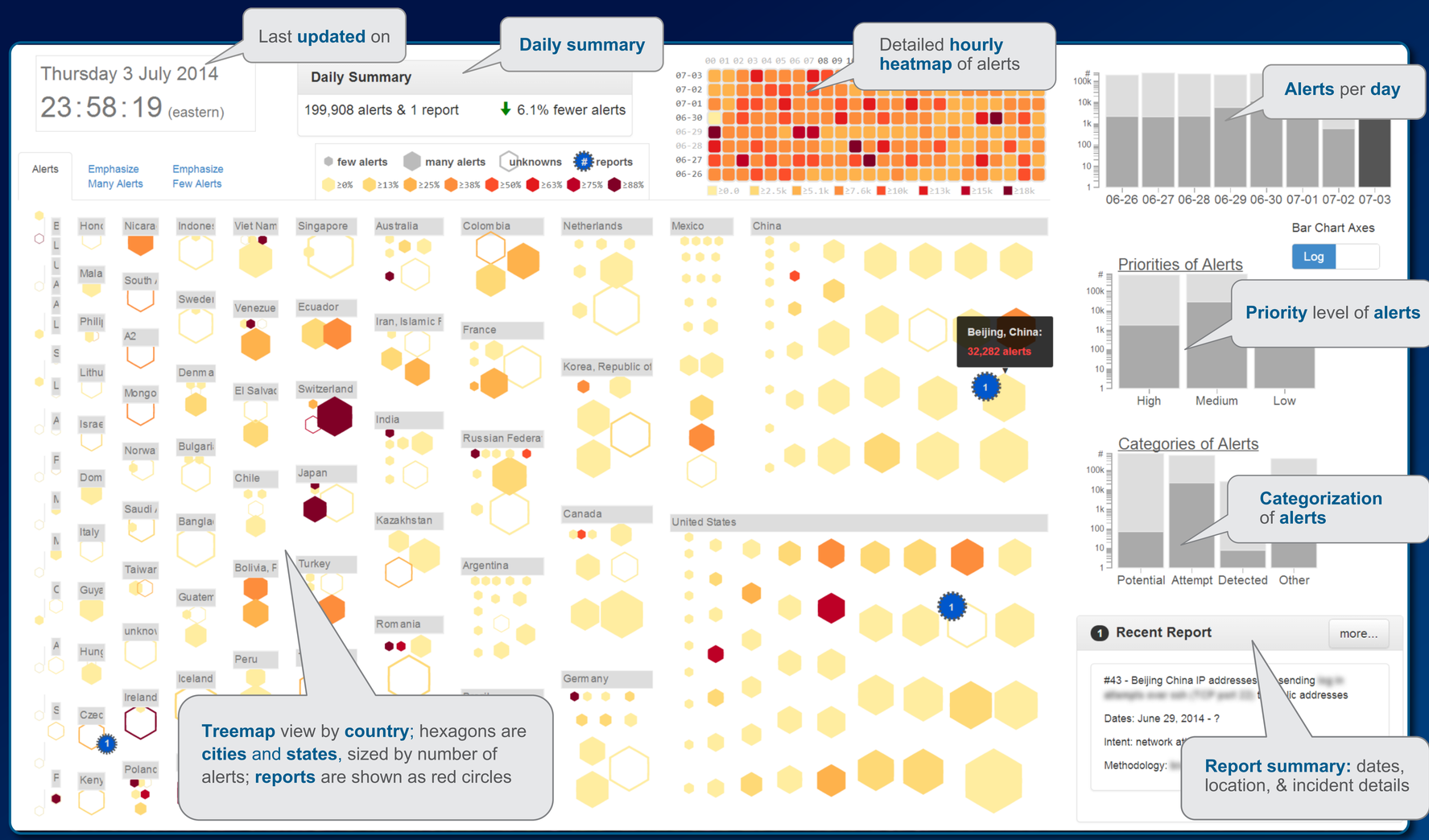
NOC Manager (information-synthesis)

Goals	Communicate impact on operations	
Knowledge	Operations ●○○○○	Cyber ●○○○○
Cyber SA	Attention ●●●○○	Temporal Window ◄——►
Key Questions	• Does this attack matter? • How serious is the attack? • What do I do about the attack? • Are there any negative effects?	• How successful was the attack? • What did the bad guys do? • What did the bad guys take?

Information

Cyber Analyst (information-gathering)

Goals	Identify anomalous network behavior	
Knowledge	Operations ●○○○○	Cyber ●●●●●
Cyber SA	Attention ●●●●○	Temporal Window ◄——►
Key Questions	• What does my network look like? • What happened on the network • last night? What's different? • Is something bad happening?	• How was my network attacked? • Who is attacking my network? • Does this attack matter? • What did the bad guys do?



Scenarios

Scenarios aided us to build our prototype for crafting stories

- Status: daily status of operations
  - "Green" status: non-critical updates; scheduled maintenance
  - "Red" status: critical vulnerabilities; hardware/software failures
- Event: report of an attacker that downloaded information
- Trend: detecting correlated events from other reports or alerts

Sources of Data

DATA	*SOURCE*
Geolocation	MaxMind Database (IPs)
Reports	IT Security Analyst
Alerts	External Network – IDS system

External Traffic from **Around the Globe**

Detailed Information on **Two Recent Incidents**

Millions of Alerts

MIT Lincoln Laboratory Acknowledgements: Diane Staheli, Martine Kalke, Matt Leahy, Rick Larkin, Maureen Hunter, Raul Harnasch, Tamara Yu, David O'Gwynn, Scott Macdonald, Bill Young, Roop Ganguly and Chris Degni

This work is sponsored by Office of the Secretary of Defense under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.