Sean McKenna, Diane Staheli<sup>\*</sup>, Cody Fulcher<sup>\*</sup>, Miriah Meyer \* MIT Lincoln Laboratory

# Cyber analysts protect computer networks from information theft and denial of service.

Information

## CEO (decision-making) **Coordinate personnel and operations** Goals Cyber Operations Knowledg Temporal Window 0000 Cyber SA • How can we maintain ongoing operations? • What could happen if a critical system is impacted? Key Questions 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)** Maintain cyber situational awareness Goals Operations Cyber Knowled Temporal Window Cyber S/ • What did the bad guys do/take? Does this attack matter? • Is it a good day on the network? • How serious is the attack? Key Questions • How is my network different • What do I do about the attack? • from last week? Are there any negative effects?

NOC Manager (information-synthesis			
Goals	Communicate impact on operations		
Knowledge	Operations	Cyber	
Cyber SA	Attention	Temporal Window	
Key Questions	<ul> <li>Does this attack matter?</li> <li>How serious is the attack?</li> <li>What do I do about the attack?</li> <li>Are there any negative effects?</li> </ul>	<ul> <li>How successful was the attack?</li> <li>What did the bad guys do?</li> <li>What did the bad guys take?</li> </ul>	

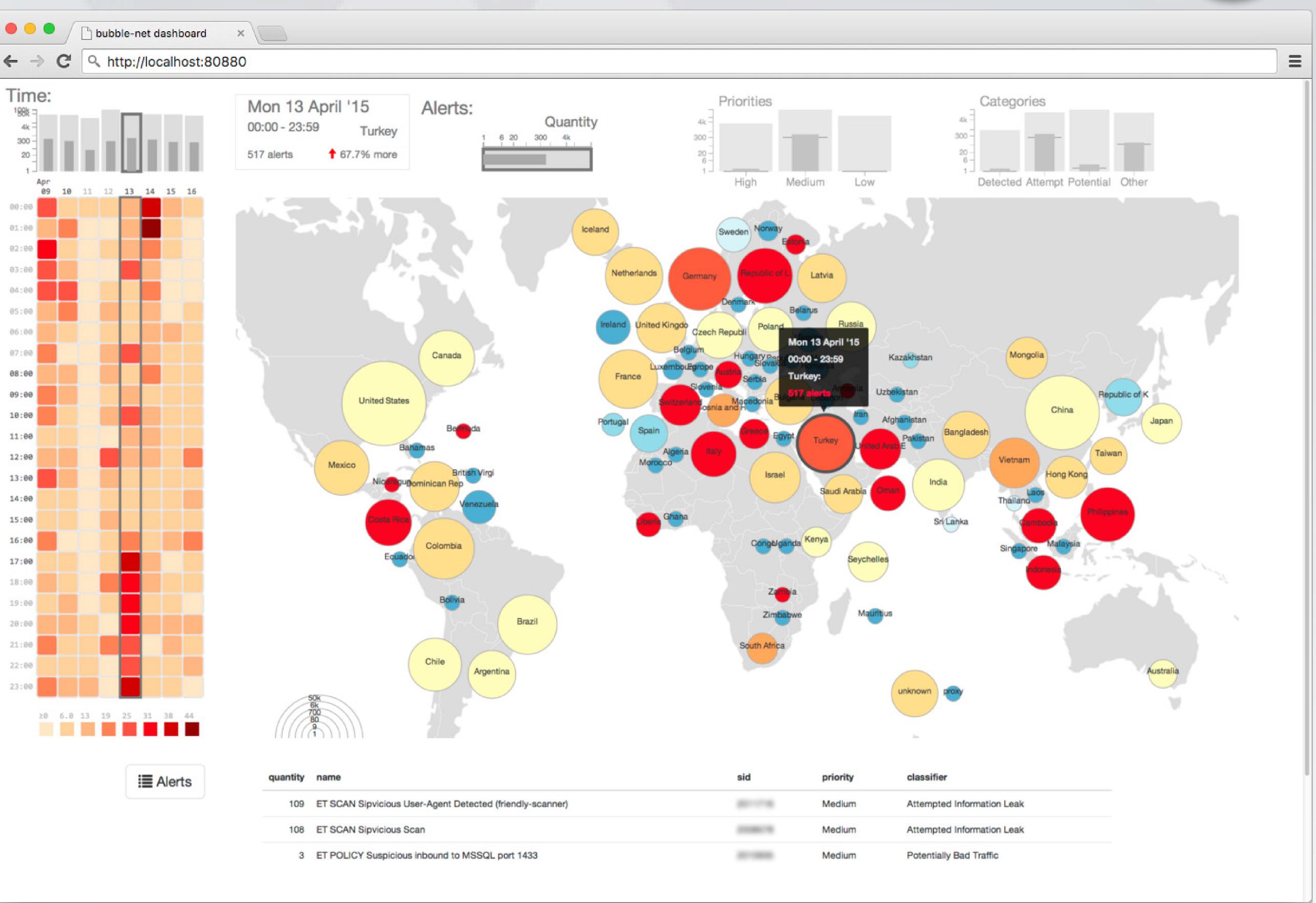
Cyber Analyst (information-gathering)			
Goals	Identify anomalous network behavior		
Knowledge	Operations	Cyber	
Cyber SA	Attention	Temporal Window	
Key Questions	<ul> <li>What does my network look like?</li> <li>What happened on the network</li> <li>last night? What's different?</li> <li>Is something bad happening?</li> </ul>	<ul> <li>How was my network attacked?</li> <li>Who is attacking my network?</li> <li>Does this attack matter?</li> <li>What did the bad guys do?</li> </ul>	

Acknowledgements: Jonzy, Dan Bowden, Tamara Denning, and staff members at MIT Lincoln Laboratory for the personas method. This work is sponsored in part by the Air Force Research Laboratory and the DARPA XDATA program. The Lincoln Laboratory portion of this work was sponsored by the Assistant Secretary of Defense for Research & Engineering under Air Force Contract FA8721-05- C-0002. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the United States Government.



**BubbleNet: A Cyber Security Dashboard** 

With personas, designers can build systems to meet the needs of many kinds of users.



# Utilizing these personas, we obtained tasks such as discovering and communicating patterns.



