

Counter Terrorism Indications & Warning

Dr. Lisa Costa, lahc@mitre.org

Mr. Tom Carroll, tcarroll@mitre.org

Dr. Dick Moynihan, moynihan@mitre.org

813-831-5535 • lahc@mitre.org

Army-Contract MOIE

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow and orange to the left of the text.

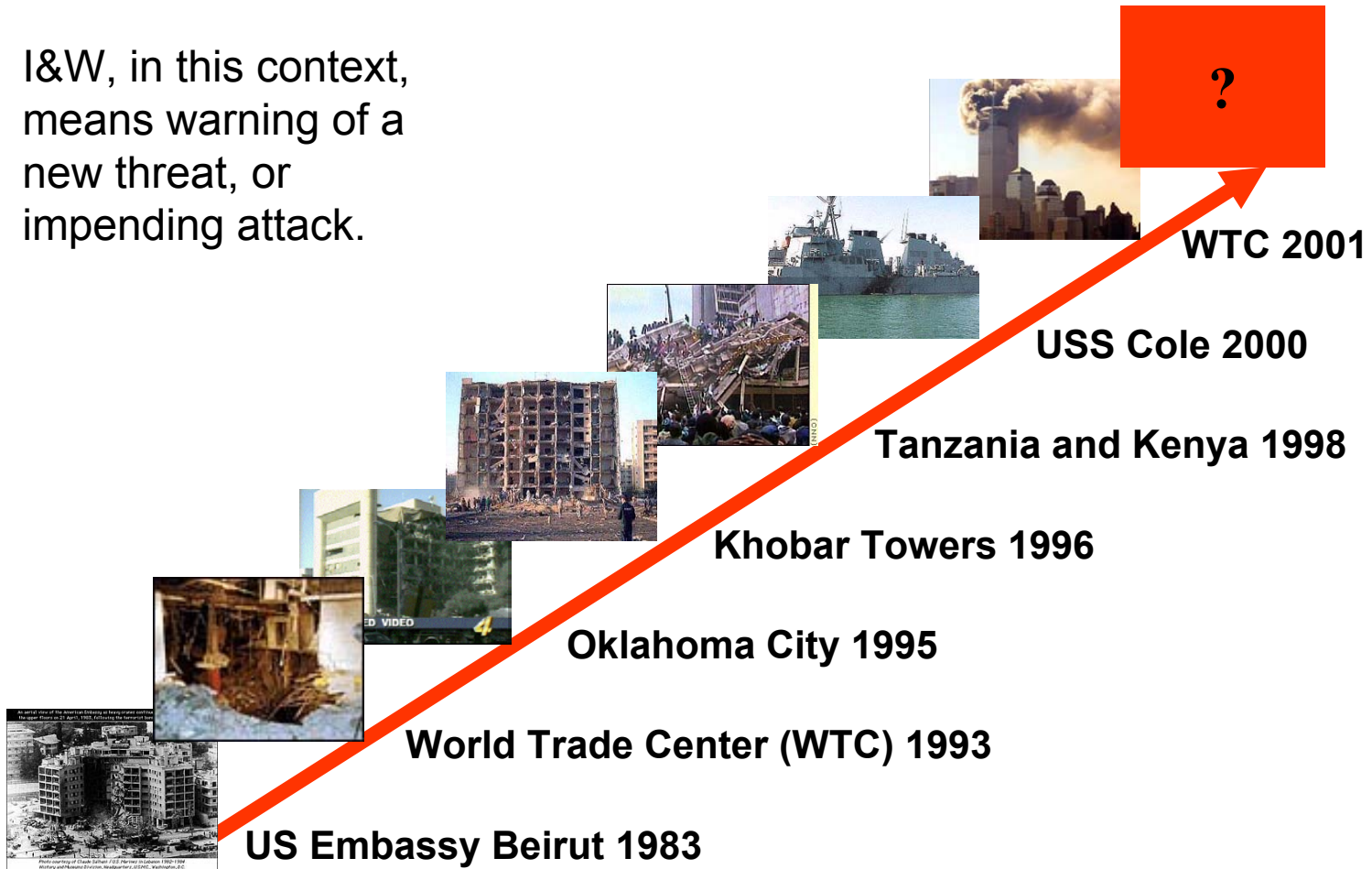
MITRE
Technology
Program

Problem

Can a well-implemented counterterrorism indications & warning model, based on advanced tools, data access, and processes, provide better I&W than current methods?

Background

I&W, in this context, means warning of a new threat, or impending attack.



Objective

- **The goal of I&W is to help prevent the next attack.**
- **The goal of this MOIE is to experiment with tools, models, processes, and data to help improve the current I&W process in the community today.**
 - **Our focus is two pronged:**
 - **Develop tools and models that help the current I&W process**
 - **Develop longer term process improvements**

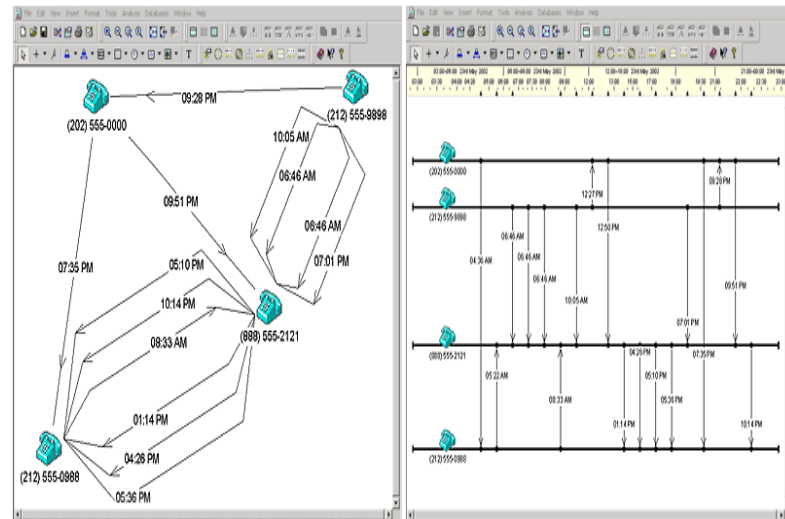
Activities

- **Develop a framework to experiment with processes, models, tools, and data with the goal of improving I&W**
 - **Understand I&W today**
 - **Use MITRE's Reference Analysis Platform for tool development and experimentation**
 - **Propose, populate, and test terrorism models**
 - **Research and evaluate analytic methods for terrorist risk prioritization**
 - **Develop tools and processes to aid CT I&W**

Highlight

- Analyze temporal differences between various terrorist attacks
- Use COTS temporal analysis tools to map same attack sequences
- Identify observables in planning, rehearsal, and execution stages
 - Map to Spec Ops Model
- Identify common traits

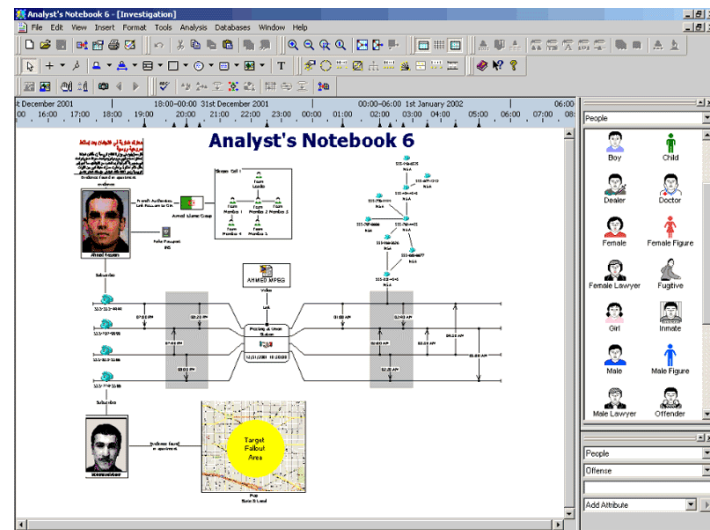
I2's Case Notebook



Highlight

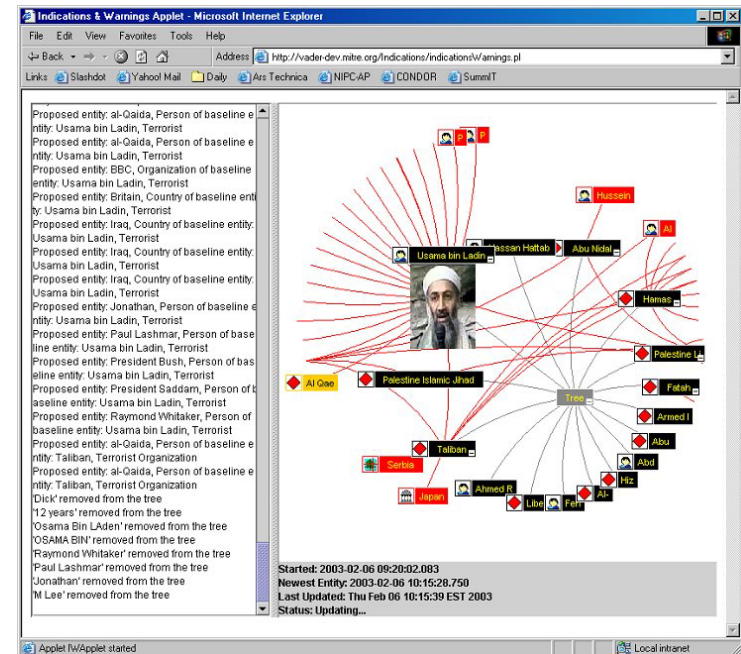
- Determine if current community link analysis efforts can be improved by adding a dynamic aspect
 - Change detection over time, geography
- Using COTS, determine data needs to support dynamic views
 - Smart entity extraction
 - User interfaces
- Determine best way to develop based on current link analysis processes

I2's Analyst Notebook



Future Plans

- Next year we propose:
 - Experimenting with our tools and processes in several CT cells across the IC
- There is a degree of risk:
 - Modeling terrorism is feasible.
 - Observables exist, but do they map to elements of terrorism models – *before* an incident?
 - Evidence to date in our work lead us to believe this is the case.



MITRE Change Detection Tool Using Inxight's VizServer