CrimeFighter: A Toolbox for Counterterrorism

Uffe Kock Wiil

Counterterrorism Research Lab

The Maersk Mc-Kinney Moller Institute
University of Southern Denmark

CTR Lab

Counterterrorism Research Lab

- Established in the Spring of 2009
  - Research goes back to 2003
- Research & Development
  - Mathematical models
  - Processes, tools, techniques, and algorithms
  - Robust prototypes
  - End-user involvement
- Focus
  - Open source intelligence
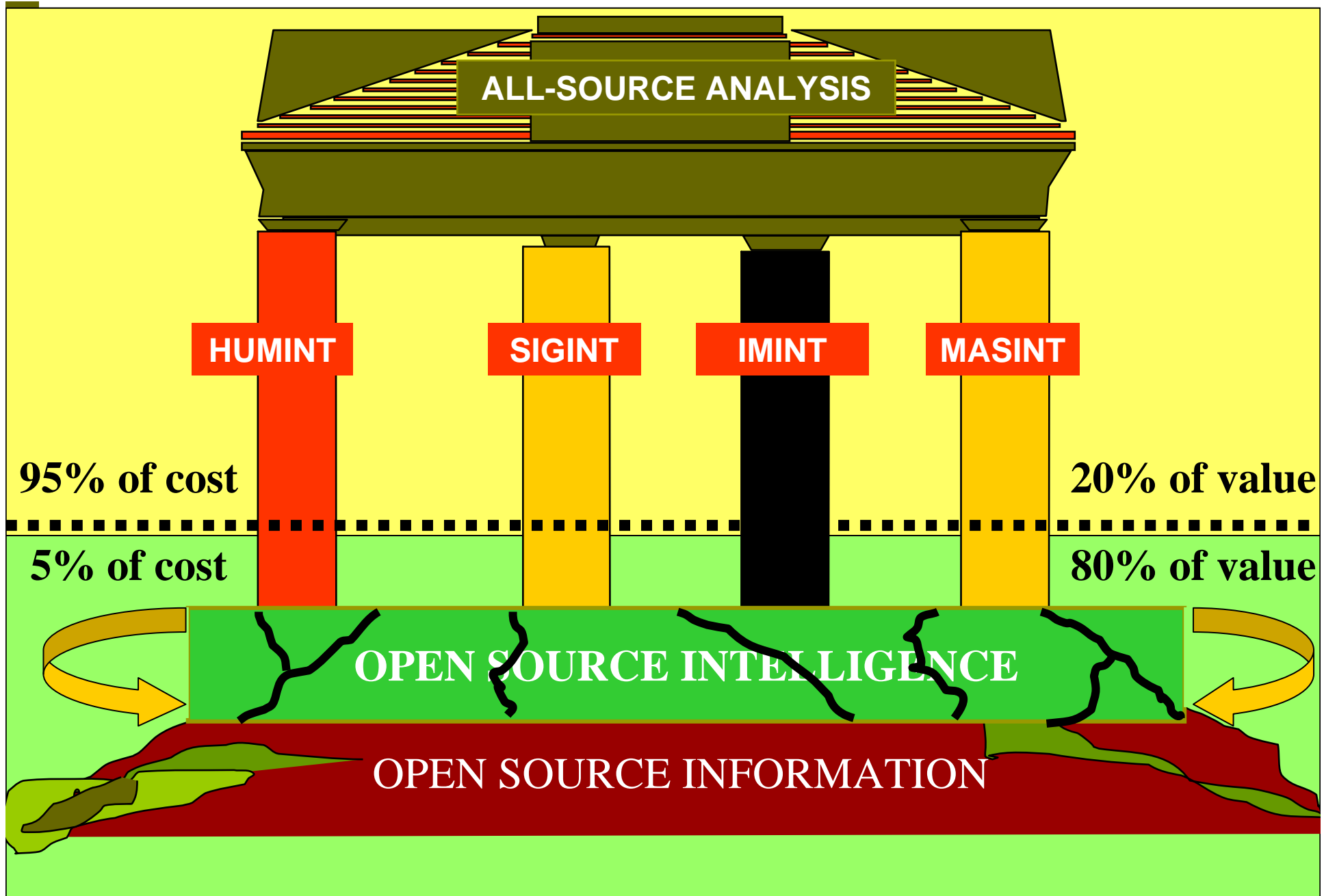 - Destabilizing terrorist networks
- 10 researchers

Counterterrorism

- Knowledge about the structure and organization of terrorist networks is important for both terrorism investigation and the development of effective strategies to prevent terrorist attacks

- Theory from the knowledge management field plays an important role in dealing with terrorist information

Open source intelligence

- Open Source Information (OSINF) is data which is available publicly – not necessarily free
- OSINF Collection is monitoring, selecting, retrieving, tagging, cataloging, visualizing & disseminating data
- Open Source Intelligence (OSINT) is proprietary intelligence recursively derived from OSINF
- OSINT is the result of expert analysis of OSINF

OSS.NET **Secret Intelligence Misses 80% of the Relevant Information!**

ALL-SOURCE ANALYSIS

HUMINT SIGINT IMINT MASINT

95% of cost 20% of value

5% of cost 80% of value

OPEN SOURCE INTELLIGENCE

OPEN SOURCE INFORMATION

KM for intelligence analysis

- Knowledge management processes, tools, and techniques can help intelligence analysts in various ways when trying to make sense of the vast amount of data being collected

- Several manual knowledge management processes can either be semi-automated or supported by software tools
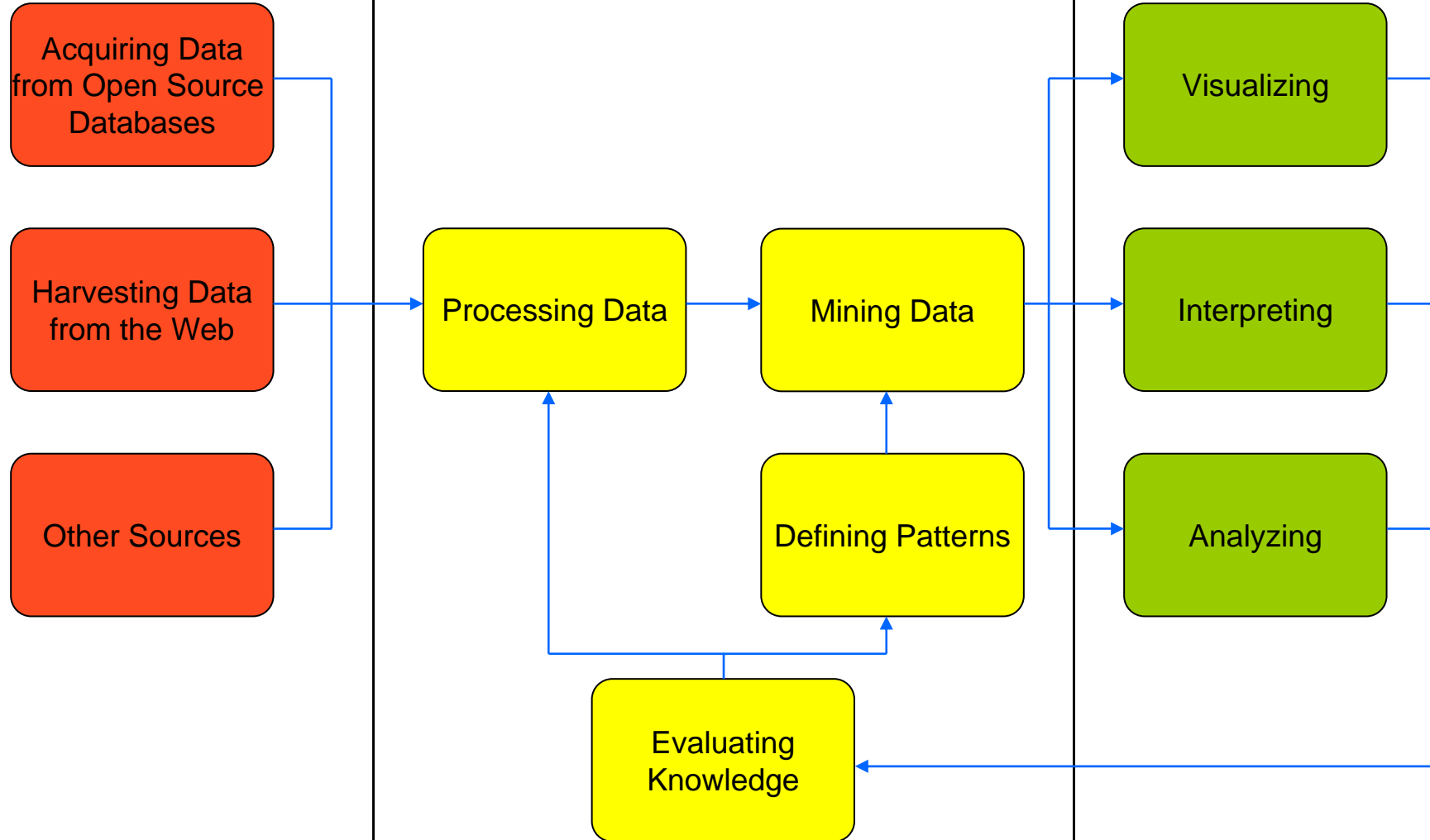
KM for intelligence analysis
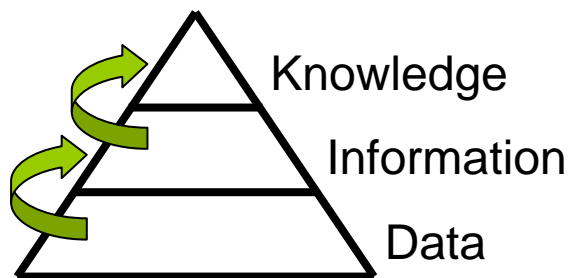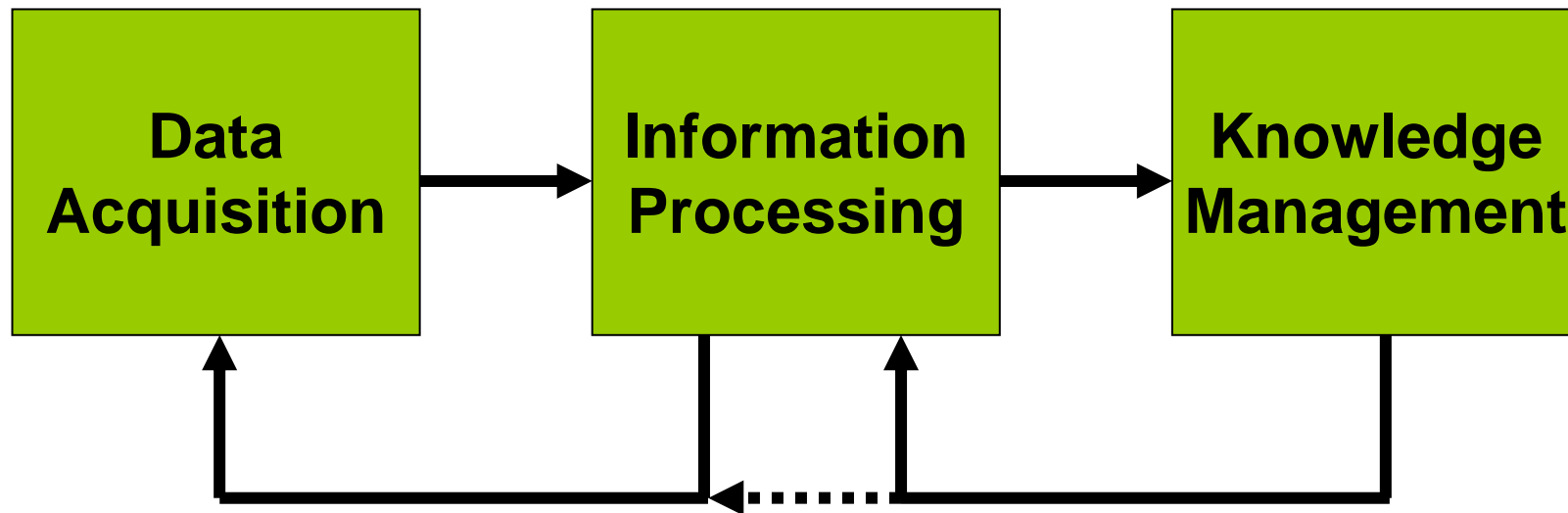
CrimeFighter

- **CrimeFighter**
  - Toolbox for counterterrorism
- **Outline**
  - KM processes in more detail
  - Related work
  - Research objectives
  - Tool categories
  - Toolbox overview
  - Previous work
  - Ongoing work
  - Contributions

Knowledge Management Processes

Data	Information	Knowledge

Acquiring Data from Open Source Databases

Harvesting Data from the Web

Other Sources

Processing Data

Mining Data

Defining Patterns

Evaluating Knowledge

Visualizing

Interpreting

Analyzing

Related work

- Counterterrorism research approaches can be divided into two overall categories
  - data collection and data modelling
- The *Dark Web Project* conducted at the AI Lab, University of Arizona (Professor Chen) is a prominent example relating to the data collection approach
- The *Networks and Terrorism Project* conducted at the CASOS Lab, Carnegie Mellon University (Professor Carley) is a prominent example relating to the data modelling approach

Related work

- CrimeFighter combines the data collection and data modelling approaches into holistic prototypes for open source intelligence

- The research is inter-disciplinary involving techniques from disciplines such as data mining, social network analysis, hypertext, visualization, and many others

- To our knowledge, no other approaches provide a similar comprehensive coverage of tools and techniques for counterterrorism
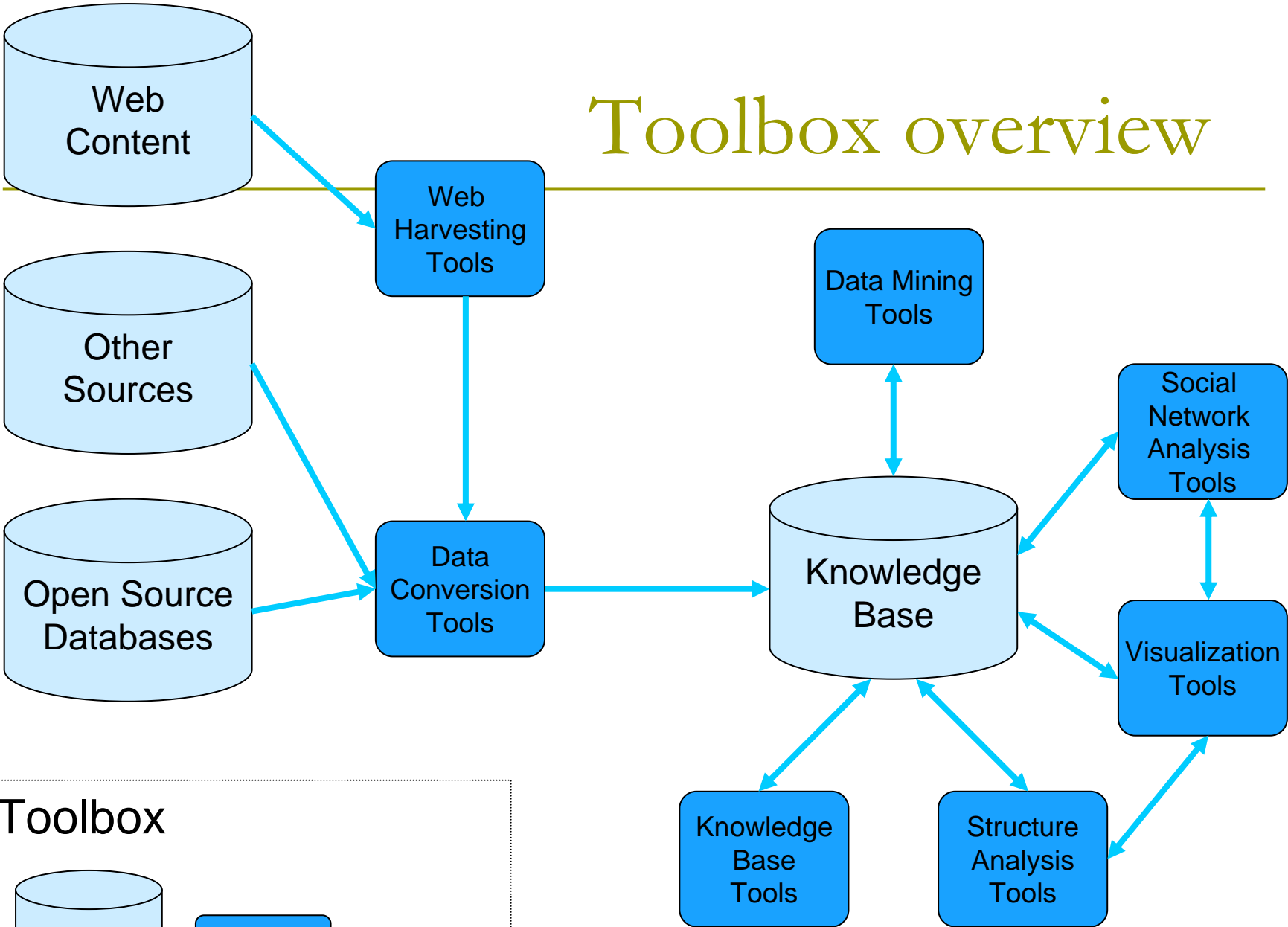
Research objectives

- To specify, develop, and evaluate novel models, algorithms, tools, and techniques for open source intelligence in close collaboration with end-users

- The tool philosophy is that the intelligence analysts are in charge and the tools are there to assist them

- The purpose of the tools is to support as many of the knowledge management processes as possible to assist the intelligence analysts in performing their work more efficiently
  - Efficient means that the analysts arrive at better analysis results much faster
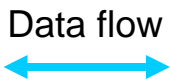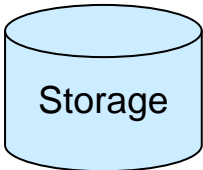
Tool categories

- Semi-automatic tools that need to be configured by the intelligence analysts to perform the dedicated task. After configuration, the tool will automatically perform the dedicated task

- Manual tools that support the intelligence analysts in performing specific tasks by providing dedicated features that enhance the work efficiency when performing manual intelligence analysis work

Toolbox overview

Web Content

Other Sources

Open Source Databases

Web Harvesting Tools

Data Conversion Tools

Data Mining Tools

Knowledge Base

Social Network Analysis Tools

Visualization Tools

Knowledge Base Tools

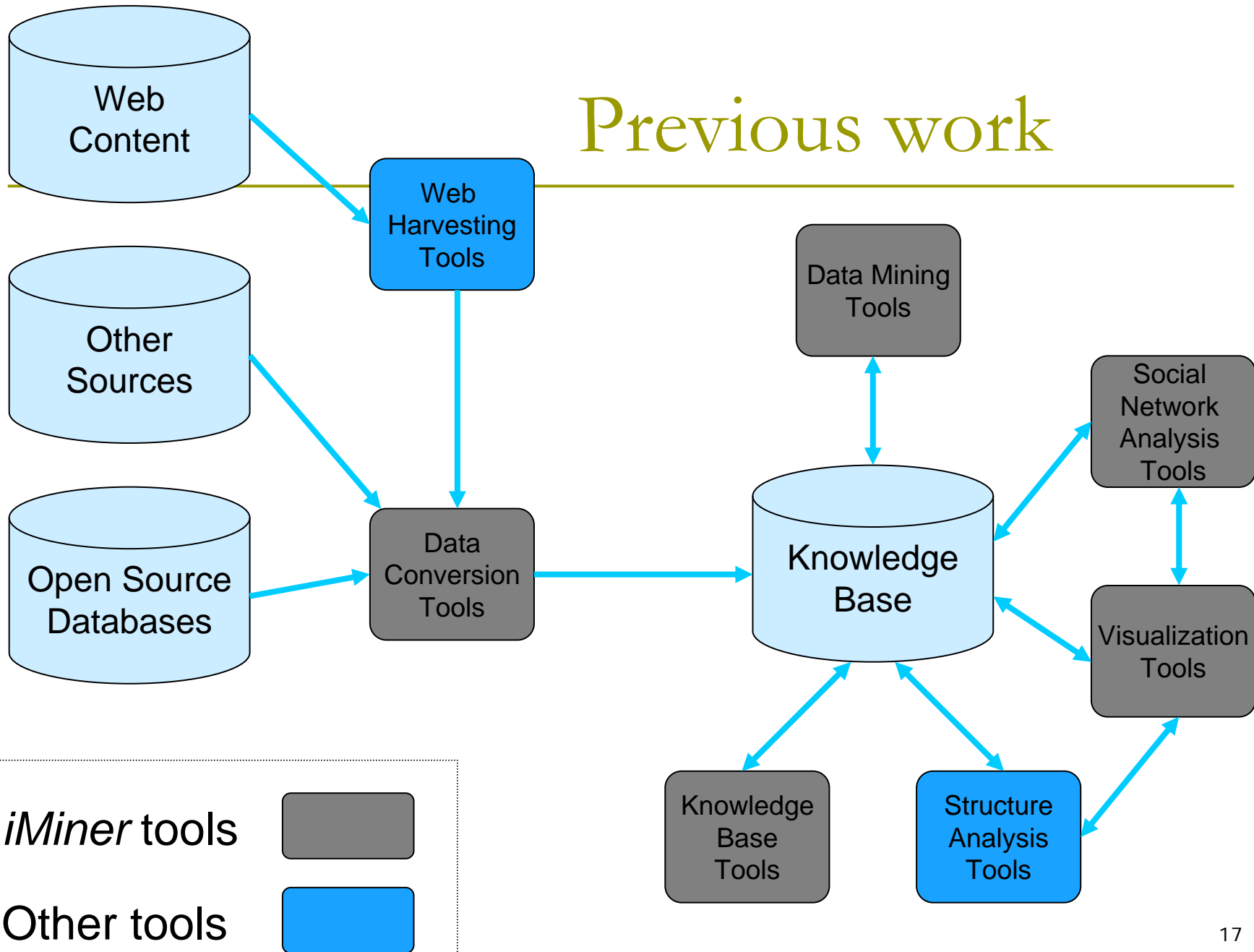Structure Analysis Tools

Toolbox

Storage

Tool

Data flow

14

Previous work

- The work on CrimeFighter builds on previous work on *iMiner*

- *iMiner* includes tools for data conversion, data mining, social network analysis, visualization, and for the knowledge base.

- *iMiner* incorporates several advanced and novel models and techniques useful for counterterrorism like subgroup detection, network efficiency estimation, and destabilization strategies for terrorist networks including detection of hidden hierarchies

Previous work

- Work has also been conducted on the ASAP tool to assist software developers to perform structural analysis of software planning data
  - Many of the spatial hypertext concepts and techniques that supports working with emergent and evolving structures used in ASAP are domain independent and can be re-used in a tool that supports intelligence analysts working with terrorist information
- Several prototypes have been constructed to harvest terrorist information from the Web
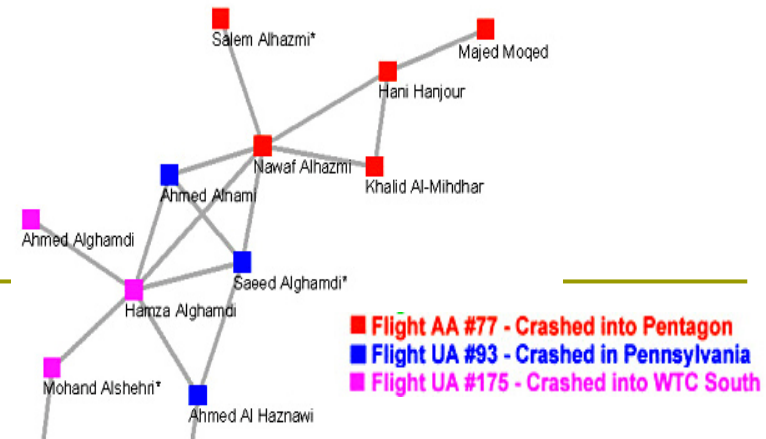 - Regular web pages
  - RSS feeds
  - Blogs

Previous work

Ongoing work

- Domain model
- Web harvesting tool
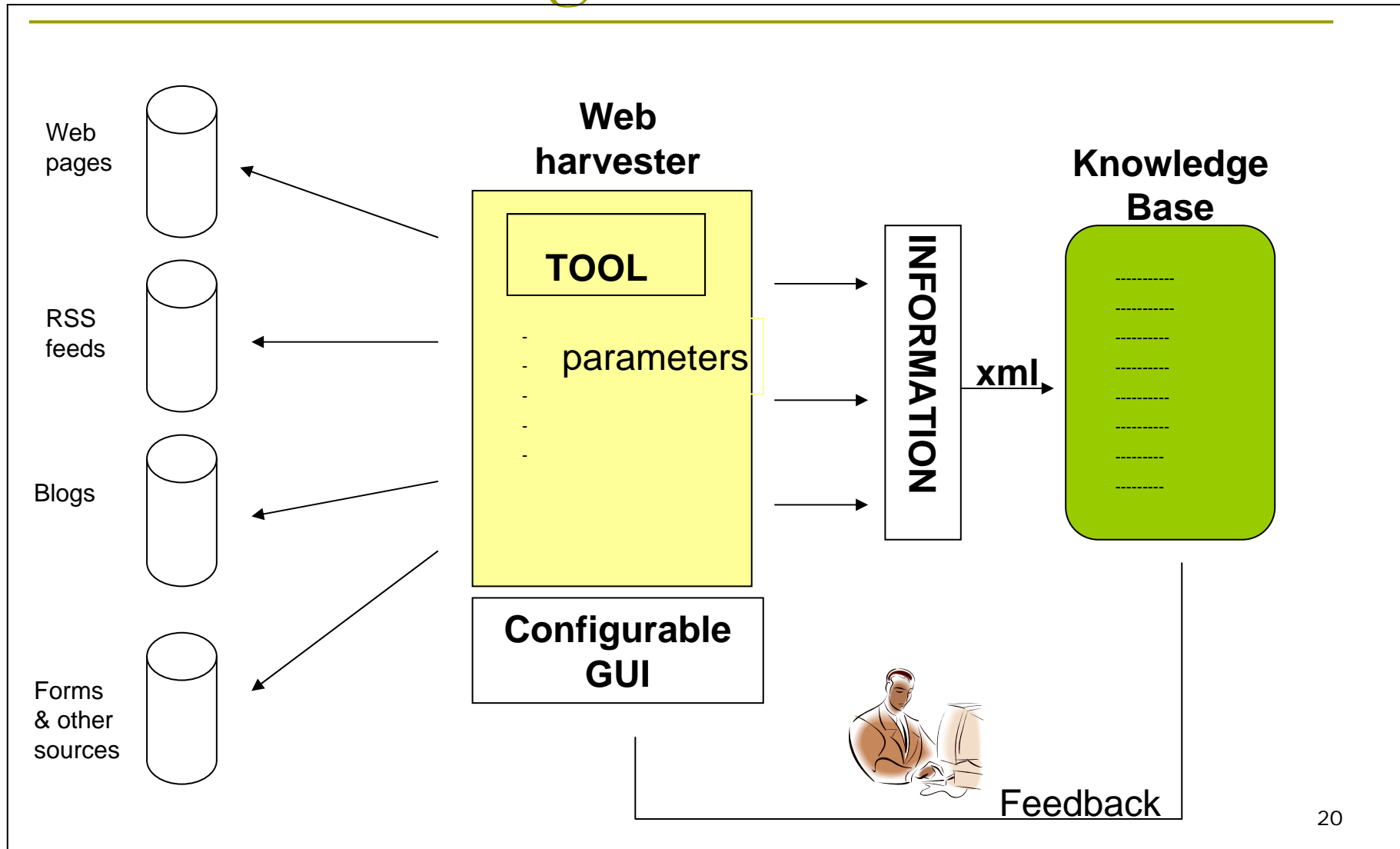- Structure analysis tool
- Software architecture

Domain model

Flight AA #77 - Crashed into Pentagon
Flight UA #93 - Crashed in Pennsylvania
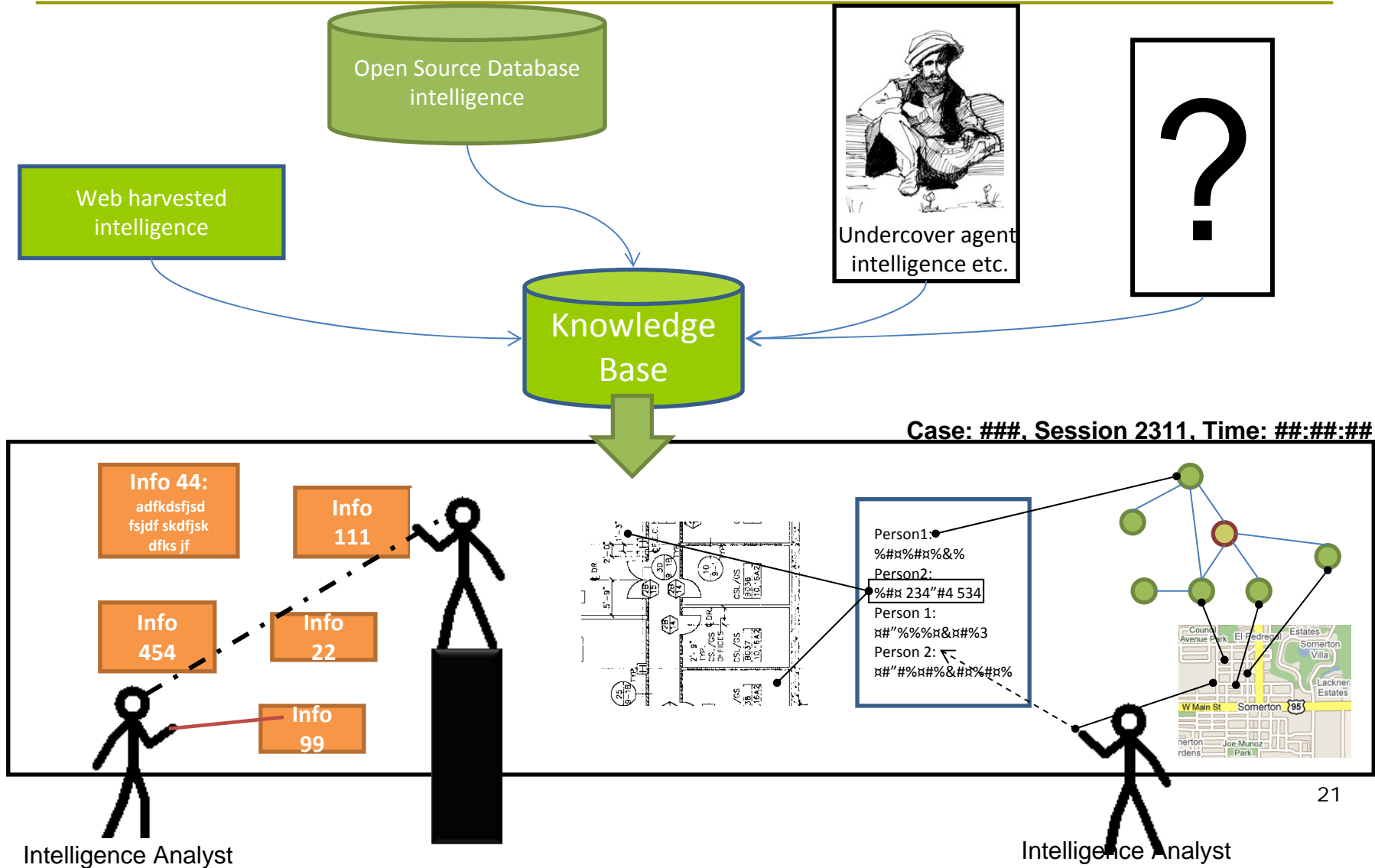Flight UA #175 - Crashed into WTC South

- ❑ **Links as first class**
  - ▪ New domain model for terrorist networks
    - ❑ Nodes and links in the graph
  - ▪ Knowledge base
    - ❑ Global Terrorism Database (GTD)
  - ▪ New social network analysis algorithms
    - ❑ Finding missing links
    - ❑ Using link weights
    - ❑ Identifying key links
  - ▪ Terrorist network visualization
    - ❑ Both nodes and links

Web harvesting tool

Web pages

RSS feeds

Blogs

Forms & other sources

Web harvester

TOOL

- parameters
-
-
-
-

Configurable GUI

INFORMATION

xml

Knowledge Base

Feedback

Structure analysis tool

Open Source Database intelligence

Web harvested intelligence

Undercover agent intelligence etc.

?

Knowledge Base

Case: ###, Session 2311, Time: ##:##:##

Info 44:
adfkdsfjsd
fsjdf skdfjsk
dfks jf

Info 111

Info 454

Info 22

Info 99

Person1:
%#¤%#¤%&%
Person2:
%#¤ 234"#4 534
Person 1:
¤#"%%%¤&¤#%3
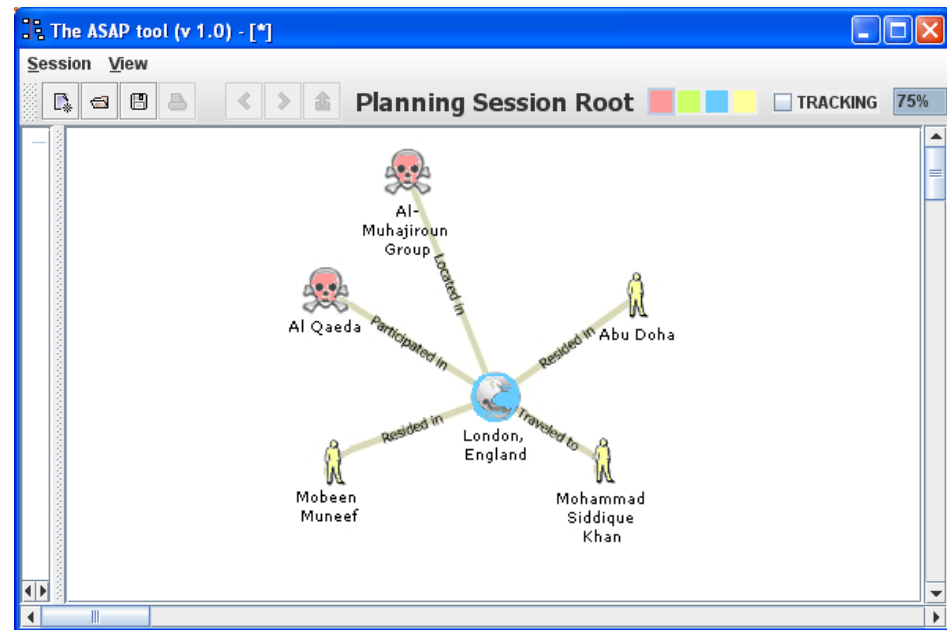Person 2:
¤#"#%¤#%&#¤%#¤%

Intelligence Analyst

Intelligence Analyst

Structure analysis tool

- Analysis tool for emergent and evolving structure of terrorist information
  - Spatial metaphor
    - Whiteboard
  - History feature
  - Session feature
  - Parser feature
  - Grouping feature

Software architecture

- Levels of integration between tools
  - Common knowledge base
  - Common domain model
  - Re-use of services

EWaS tool	SNA tool	Analysis tool
Domain model	Domain model	Domain model
Knowledge base	Knowledge base	Knowledge base
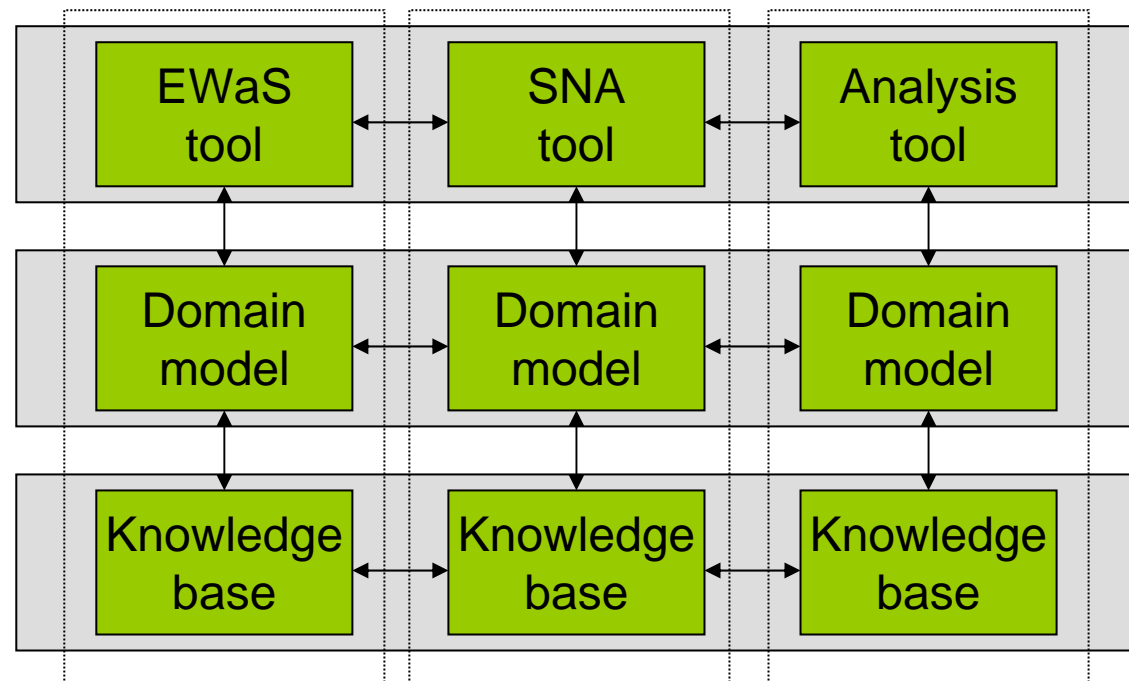
Contributions

- We have identified and described knowledge management processes, tools, and techniques that are central to the counterterrorism domain

- We have developed and implemented advanced mathematical models and software tools that help automate and support knowledge processes for counterterrorism to assist intelligence analysts in their work

- We have presented past, ongoing, and future work on CrimeFighter – a novel toolbox for counterterrorism that provides advanced support for the counterterrorism domain