Estimating Vulnerabilities in Large Covert Networks

Kathleen M. Carley

kathleen.carley@cmu.edu

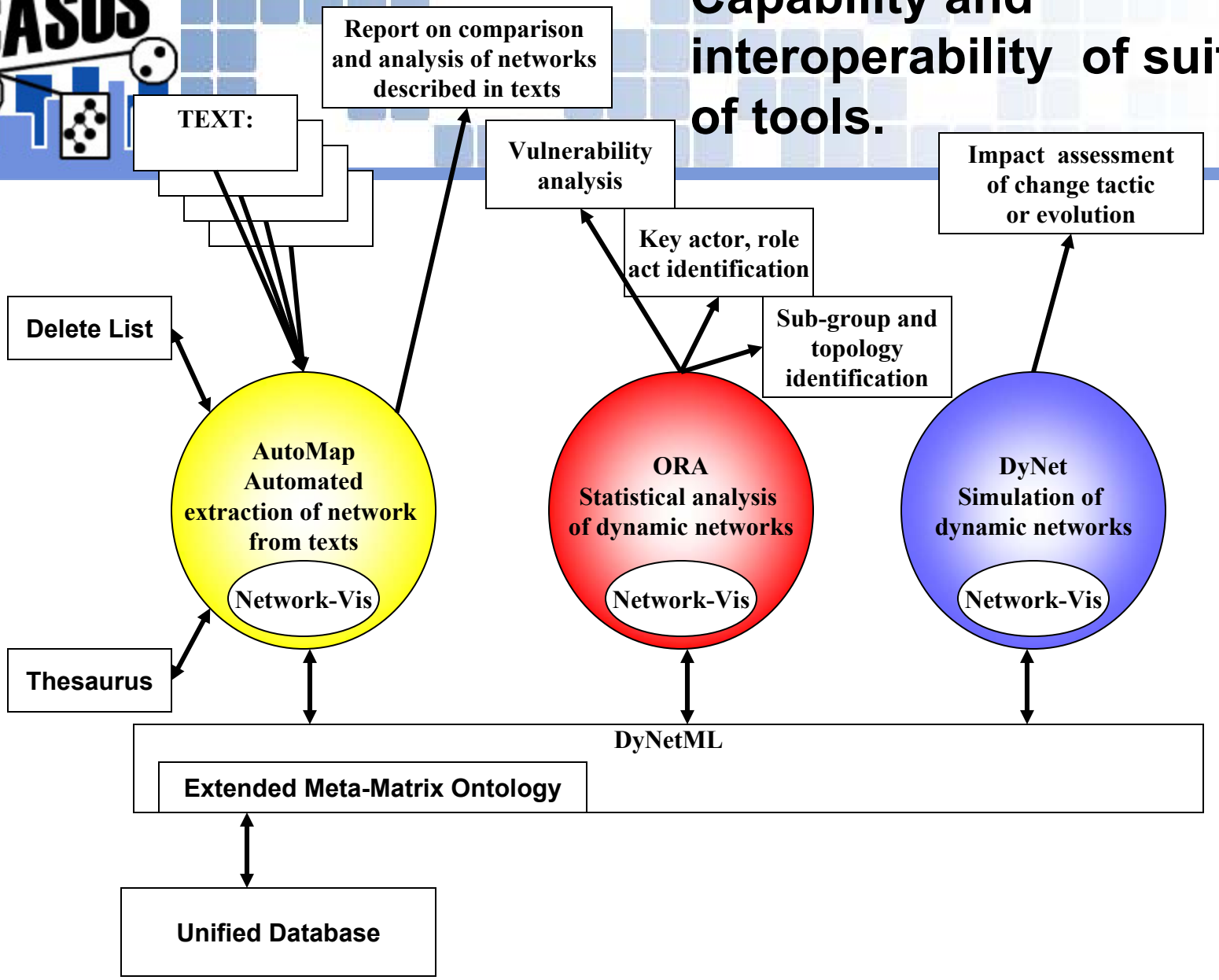
www.casos.cs.cmu.edu

412 268 6016

Overview

- Network profiles of terrorist organizations
  - Al-Quaeda
  - Hamas
  - Data derived both qualitatively and quantitatively
- Computational simulation of large-scale dynamic social networks
  - Meta-Matrix model
  - ORA Analysis
  - DyNet simulation system
- Performance of simulation tools on covert networks

Capability and interoperability of suite of tools.



Text Analysis Approach

- al Qaeda
  - Several thousand articles, web pages, etc.
  - Books
  - Data collected automatically and by hand
- Hamas
  - Several hundred articles
  - Data collected automatically and by hand

Profile: Al-Qaeda

- Built to maximize secrecy and security
  - Information partitioning between cells
  - Node and link redundancy
  - Cellular structures
    - Small, densely connected cells
    - Little interconnect between cells
      - Inter-cell connections are often dormant and only activated on the as-needed basis
    - Cells are expendable – minimizing the impact of a cell removal
  - Cell leaders are more knowledgeable then other members
  - Cell members have distributed knowledge
  - Cells are largely self-sufficient
- Absorbs local insurgencies as operational cells
- Central command structure is a 2-level hierarchy (Bin Laden and a group of top officers)
- Regional structures differ; most prevalent are cellular organizations

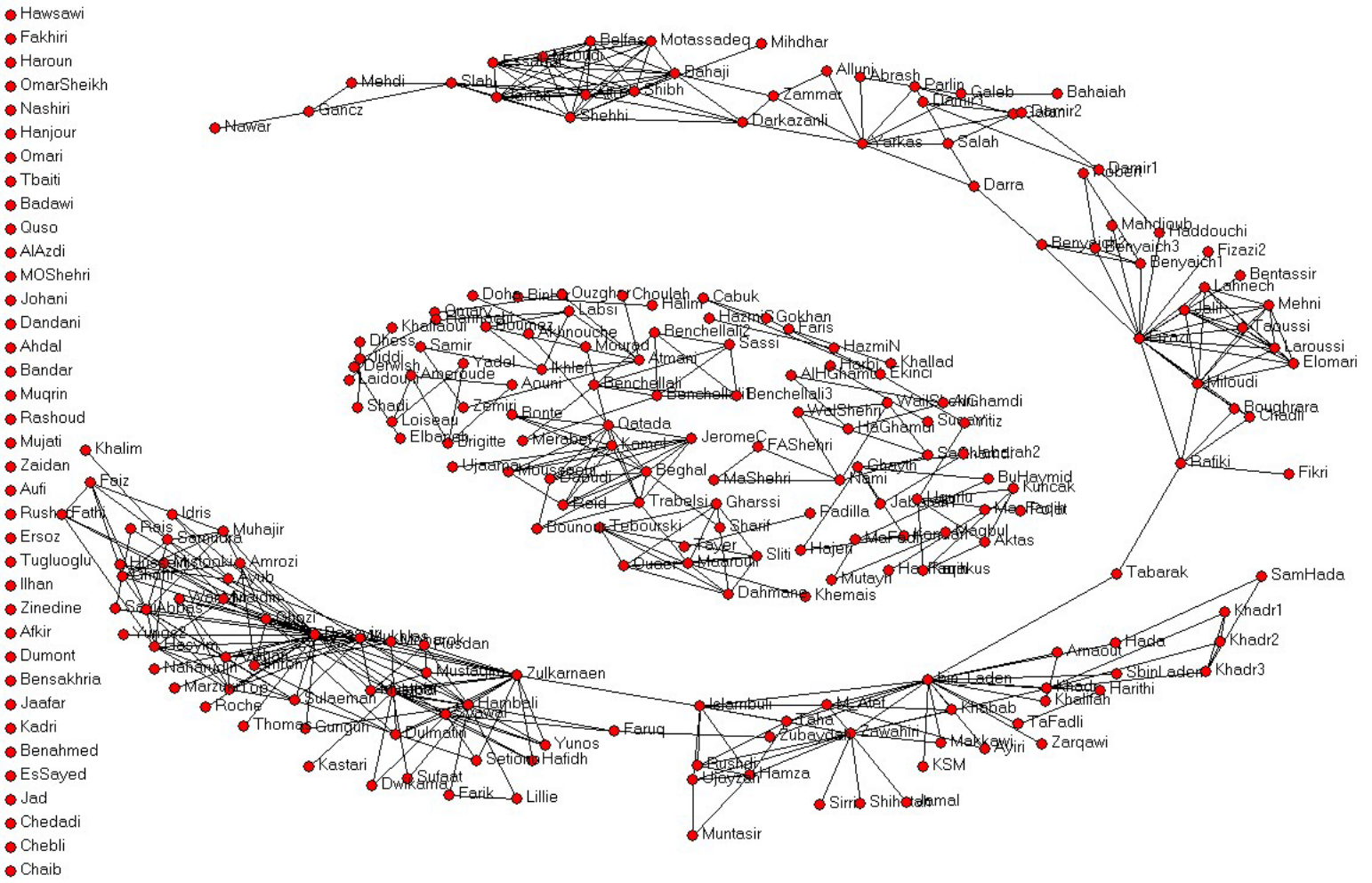
Profile: Hamas

- Hierarchical Command and Control structure
- Divided into functional "services", regionally distributed
  - "Political Wing" (based in Syria)
  - Infrastructure (local and international)
    - Social Support Infrastructure (Schools, hospitals, etc)
    - Fundraising, finance
    - Weapons procurement
    - Religious activities
  - "Military Wing"
    - Popular Uprising (organizes protests and local resistance)
    - Internal Security (Jihad Amman)
    - Suicide Bombers
    - Azzeddin Al-Quassam
      - Professional military wing
      - Trains and supplies suicide bombers

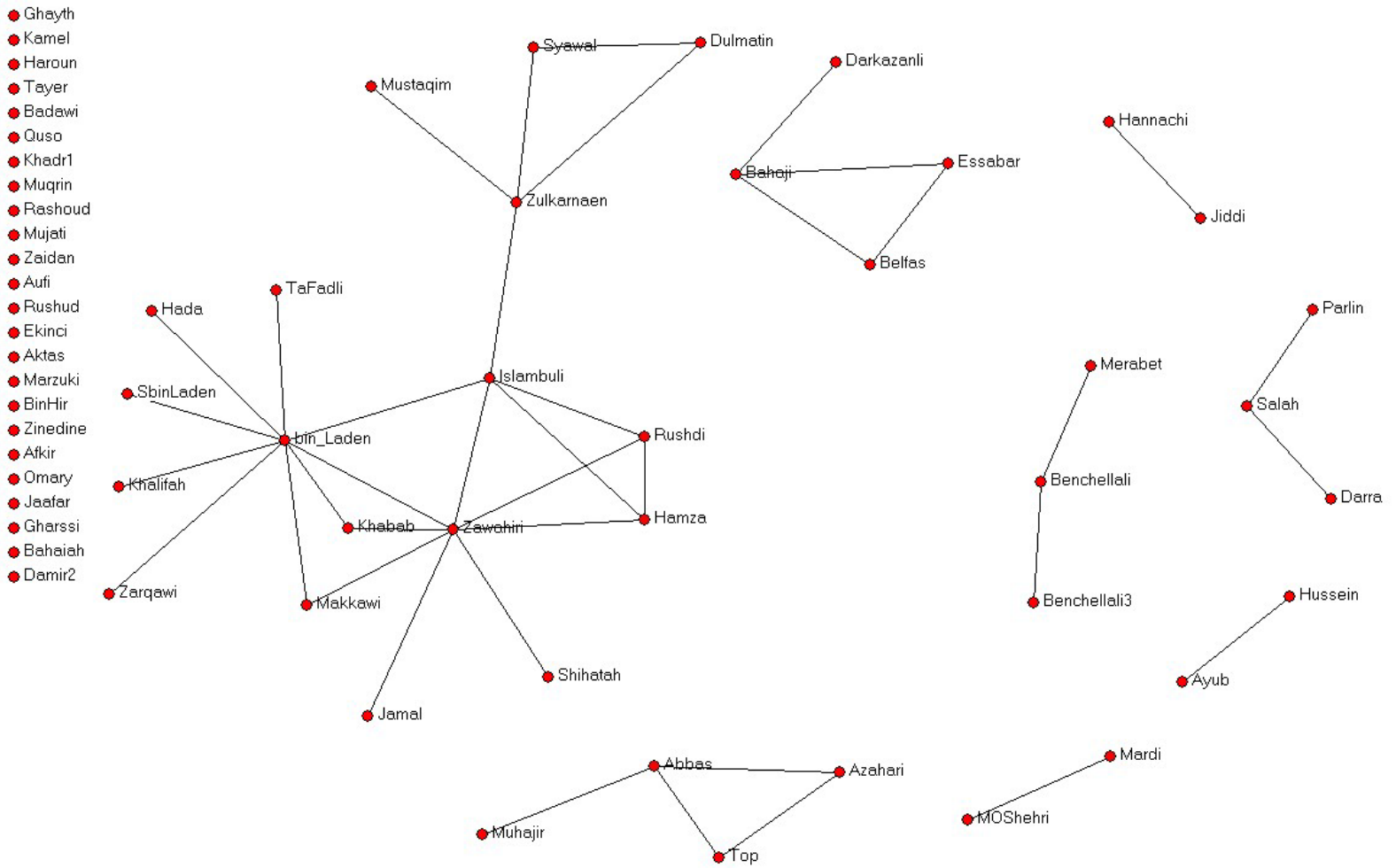
Profiles of Terrorist Networks

Feature	Al-Qaeda	Hamas
Organizational Structure	Top-level structure is a hierarchy Underlying cellular structure Absorbs structures of subsidiary groups	Matrix – by region and function
Cells	Mission-oriented Distributed skills in cell, somewhat self-sufficient	Function-Oriented Same skills in cells, need external support
Mission Structure	Cell-oriented Multiple cells cooperate for large missions	Planned by function; executed by local cells; funded regionally
Connection among cell leaders	Similarity (historical)	By function and region, also hierarchical
Executives	Cell Leaders	Functional and Regional Leaders
Integration with community	Moderate to low Hidden	Reasonably high Infrastructure - legitimate businesses Operational - infiltrated into police, etc.

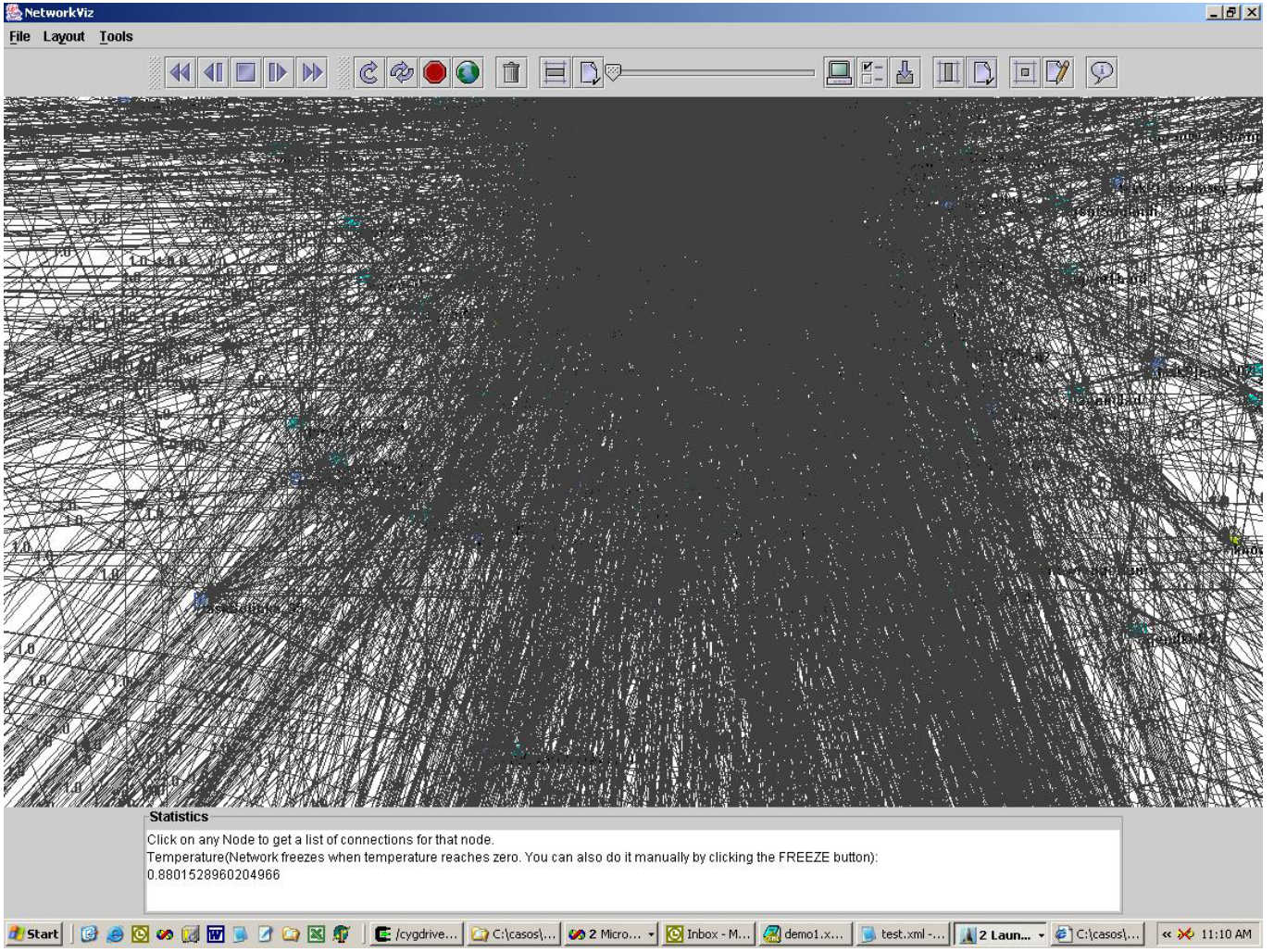
Al Qaeda 2001



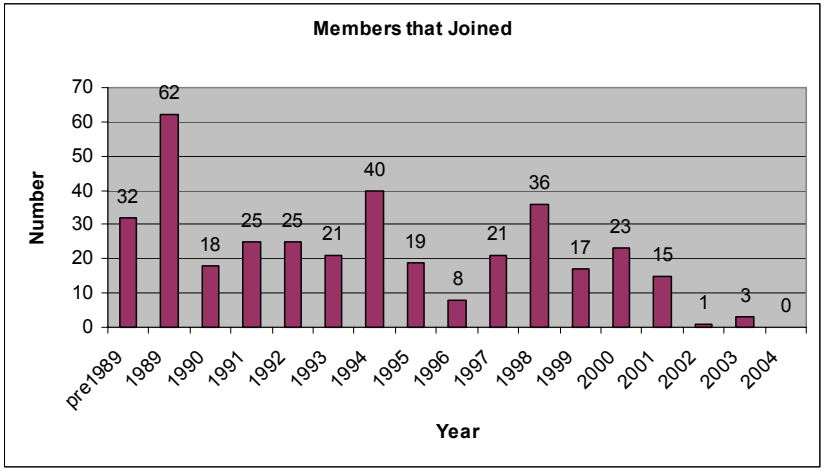
Al Qaeda 2004

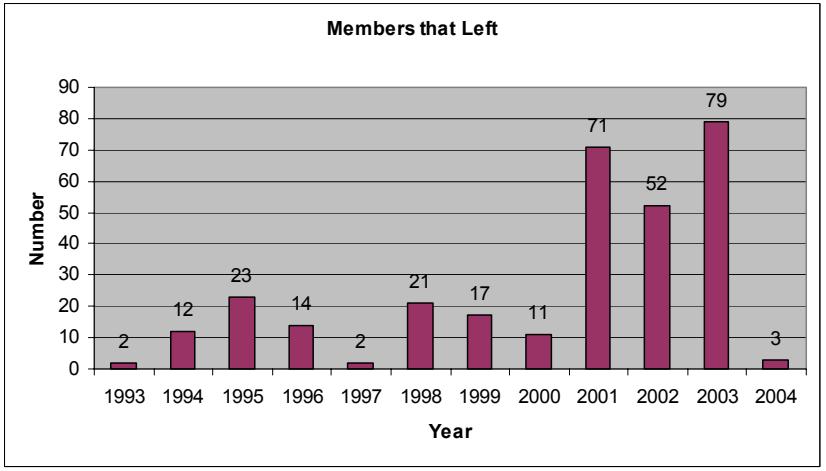


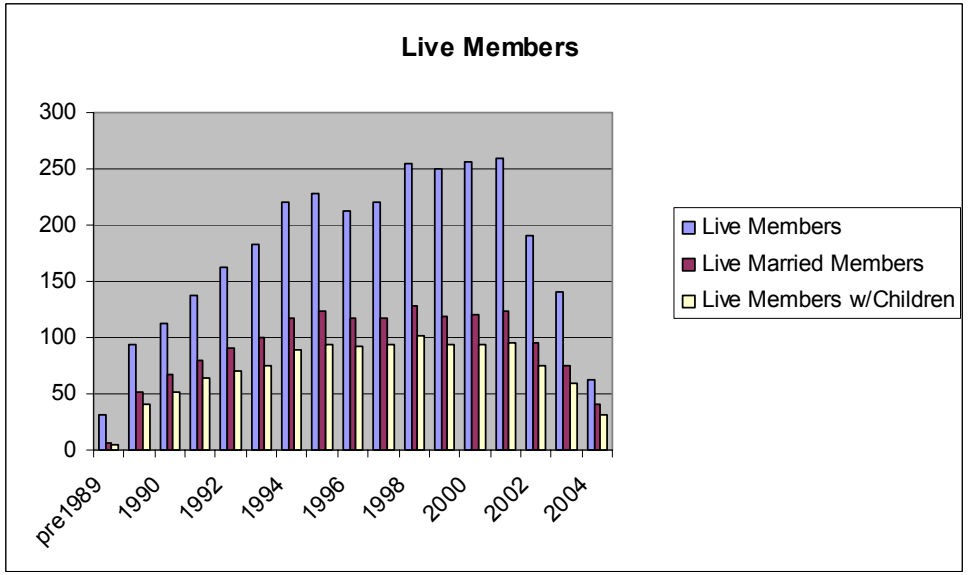
al Qaeda



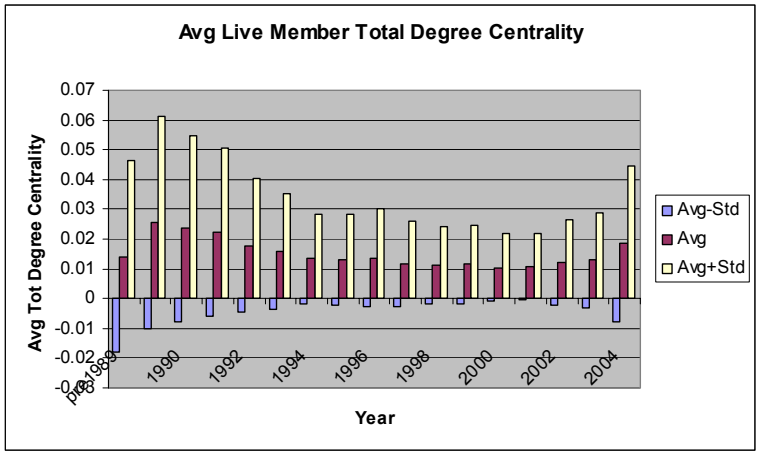
Membership

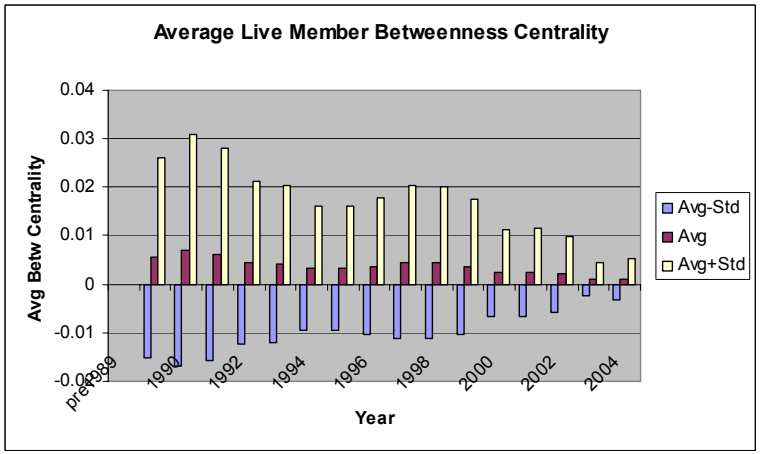


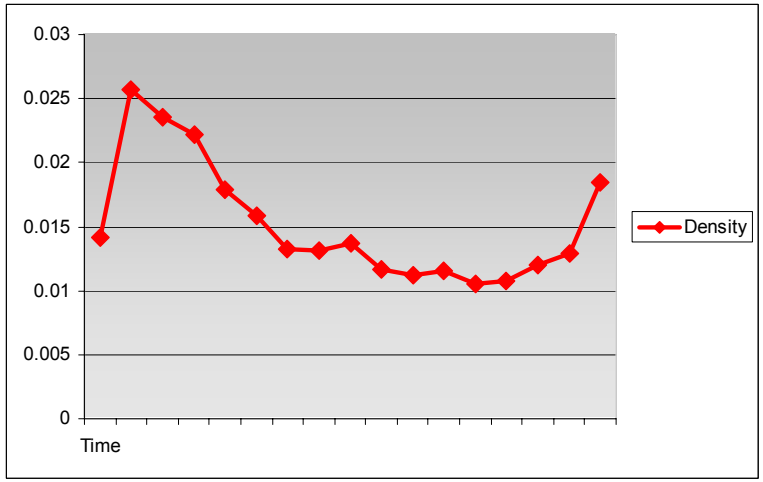


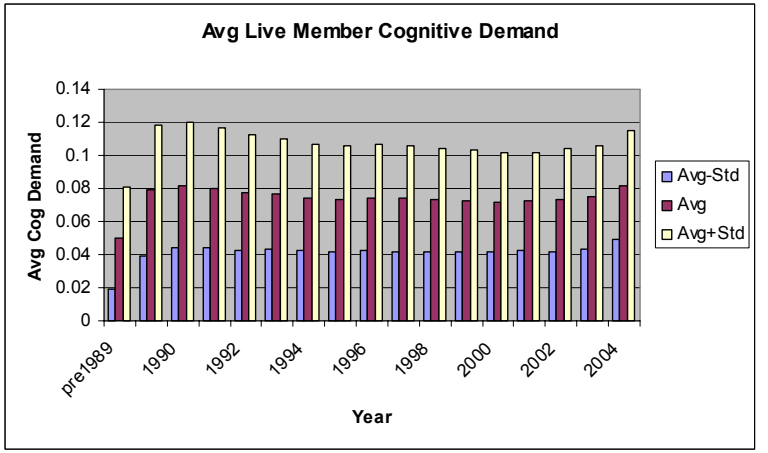


Internal Structure

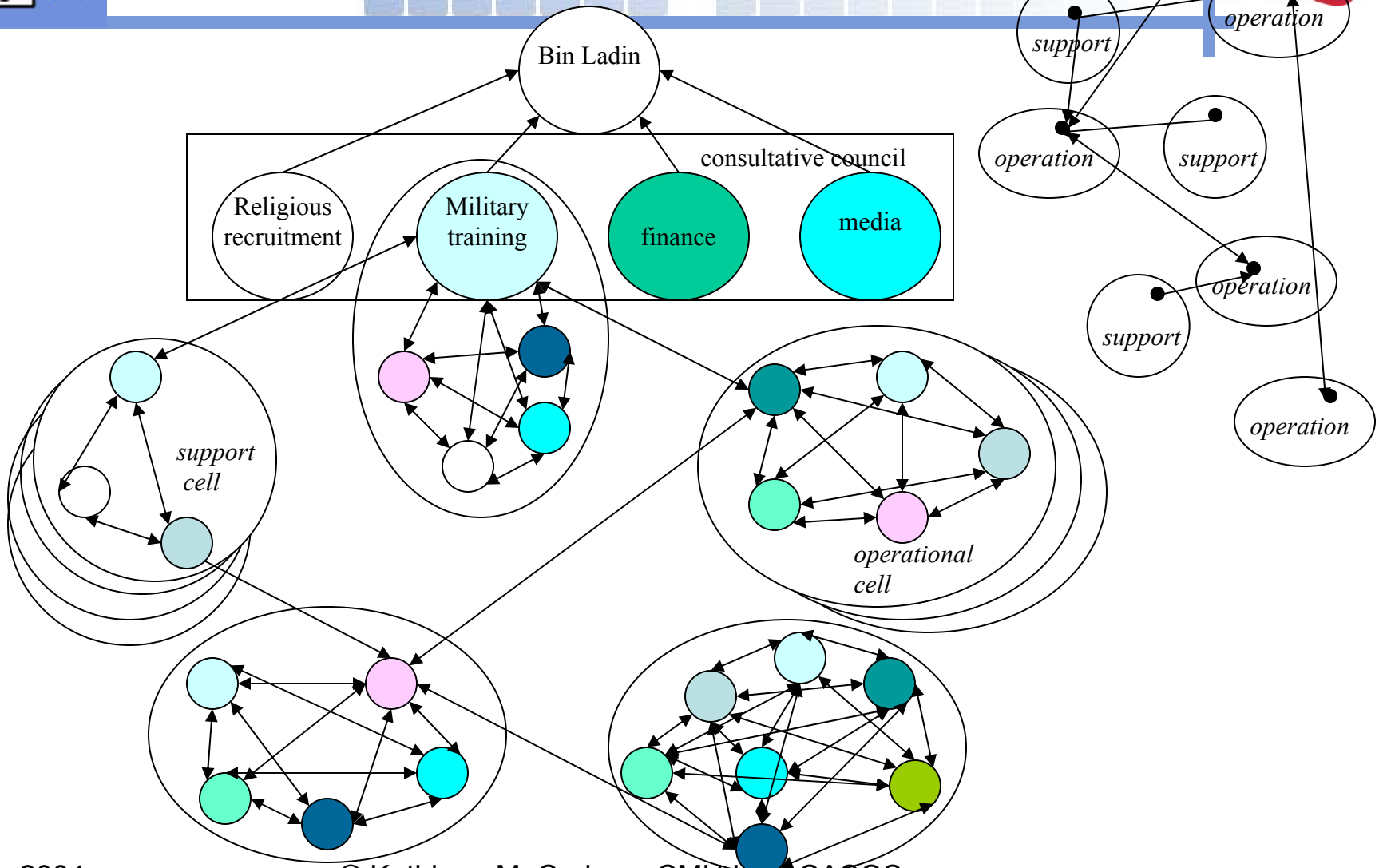




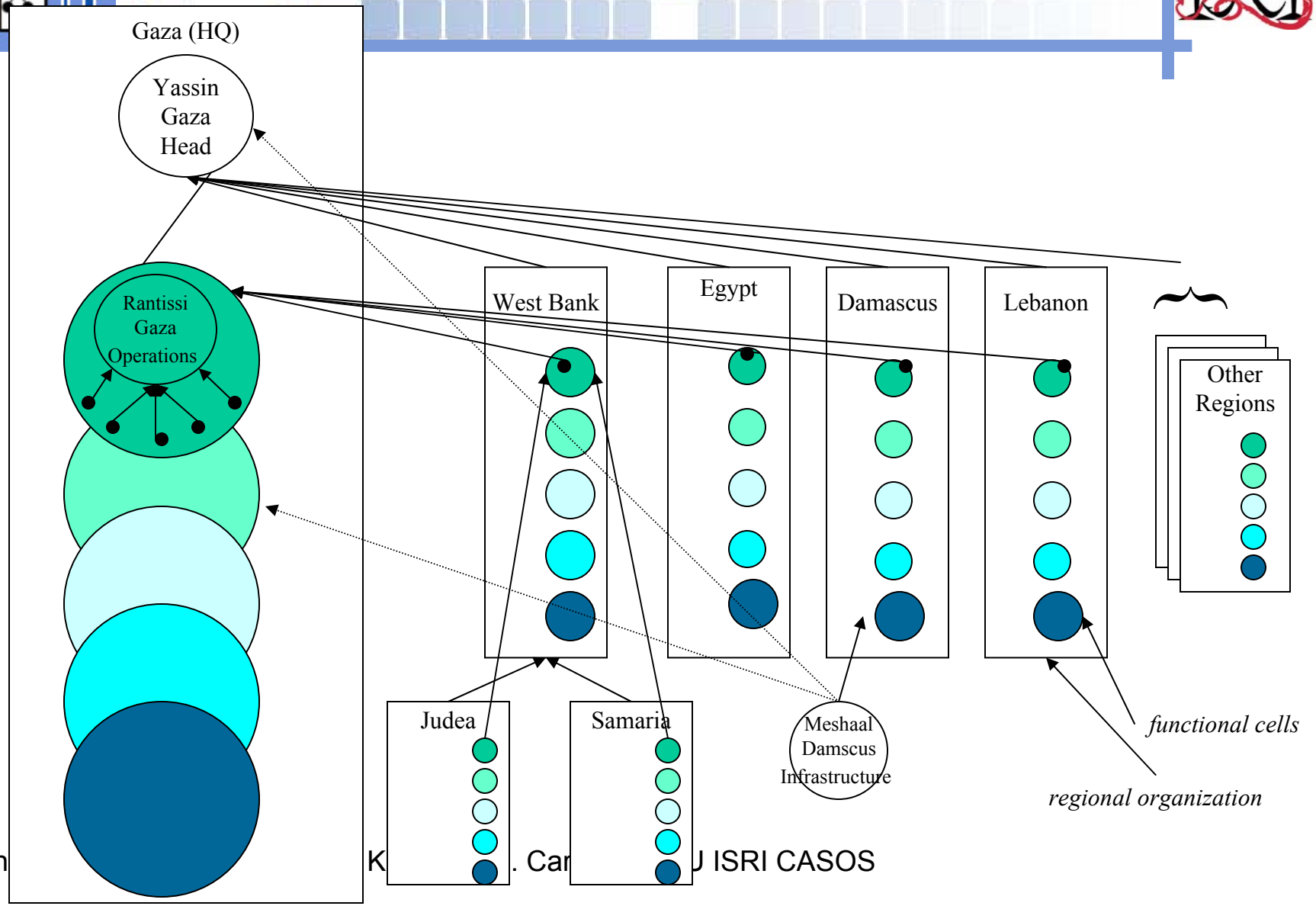




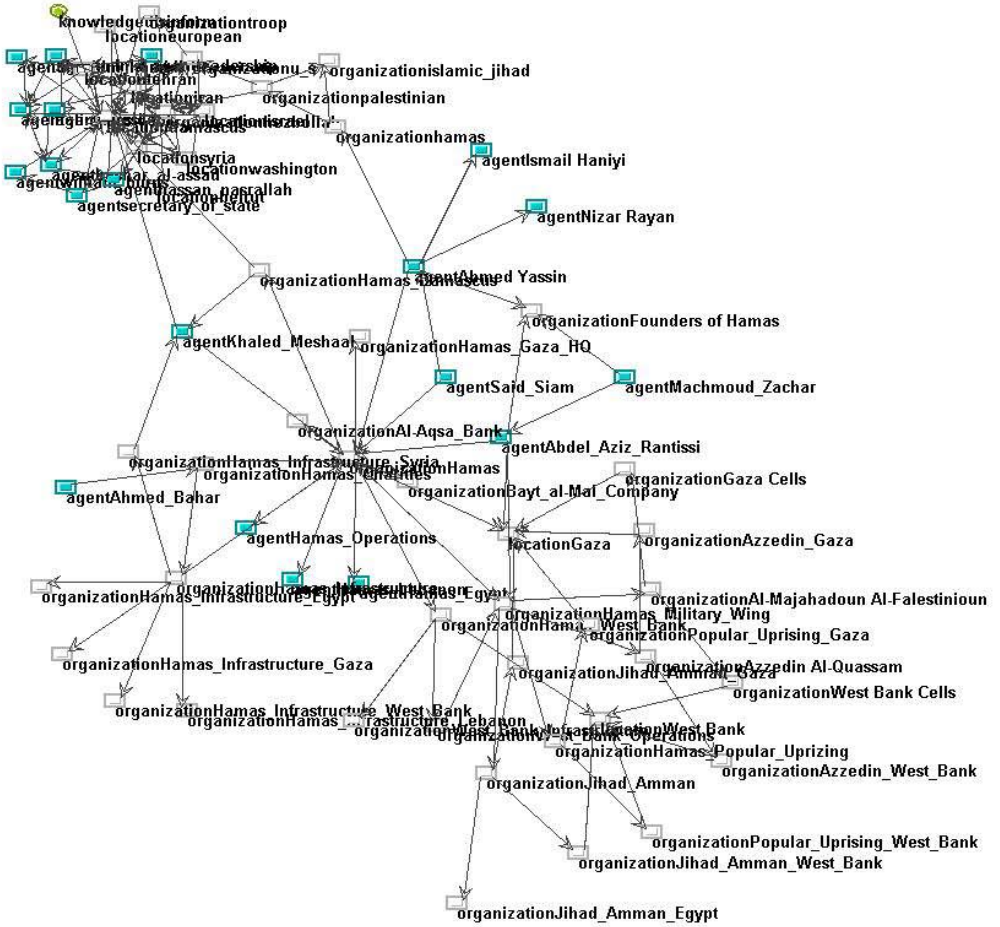
al-Qaeda



Hamas under Yassin



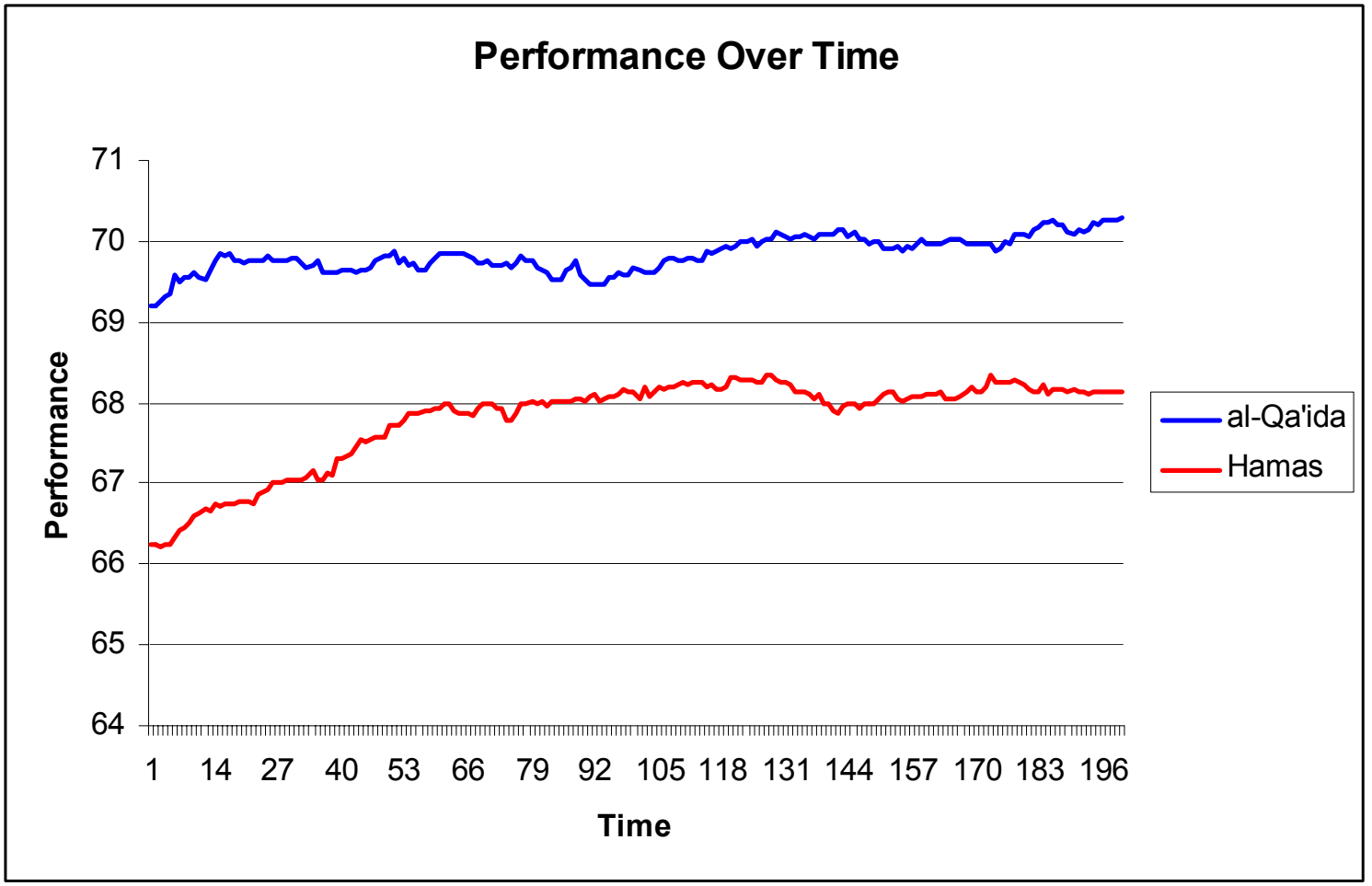
Hamas with Yassin



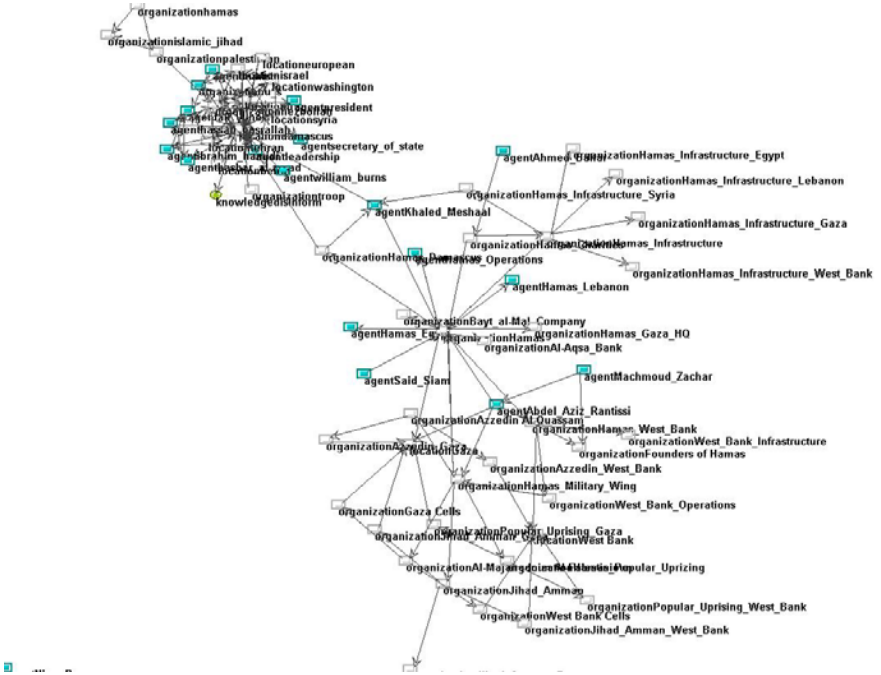
Characteristics of Key Actors

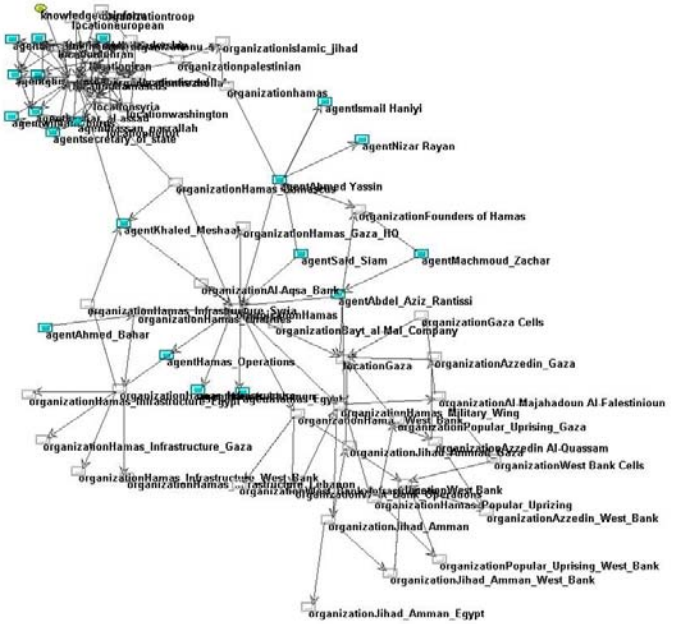
Characteristics	Meaning	al-Qa'ida	Hamas
Complexity	Very low then probably major amounts of missing data, possibly cells are self directed. Very high then system is tightly coupled and possibly prone to group think.	slightly more complex .096 Overall – very low density	slightly less complex .053 Overall – very low density
Highest in degree centrality	Individual most likely to diffuse new information, isolation of this person will be slightly crippling for a short time.	Bin Ladin .028	Yassin .011 
Highest in cognitive demand	Individual most likely to be an emergent leader, isolation of this person will be moderately crippling for a medium time	Bin Ladin .015 	Rantissi .087 

Expected Performance



Hamas Before and After Yassin

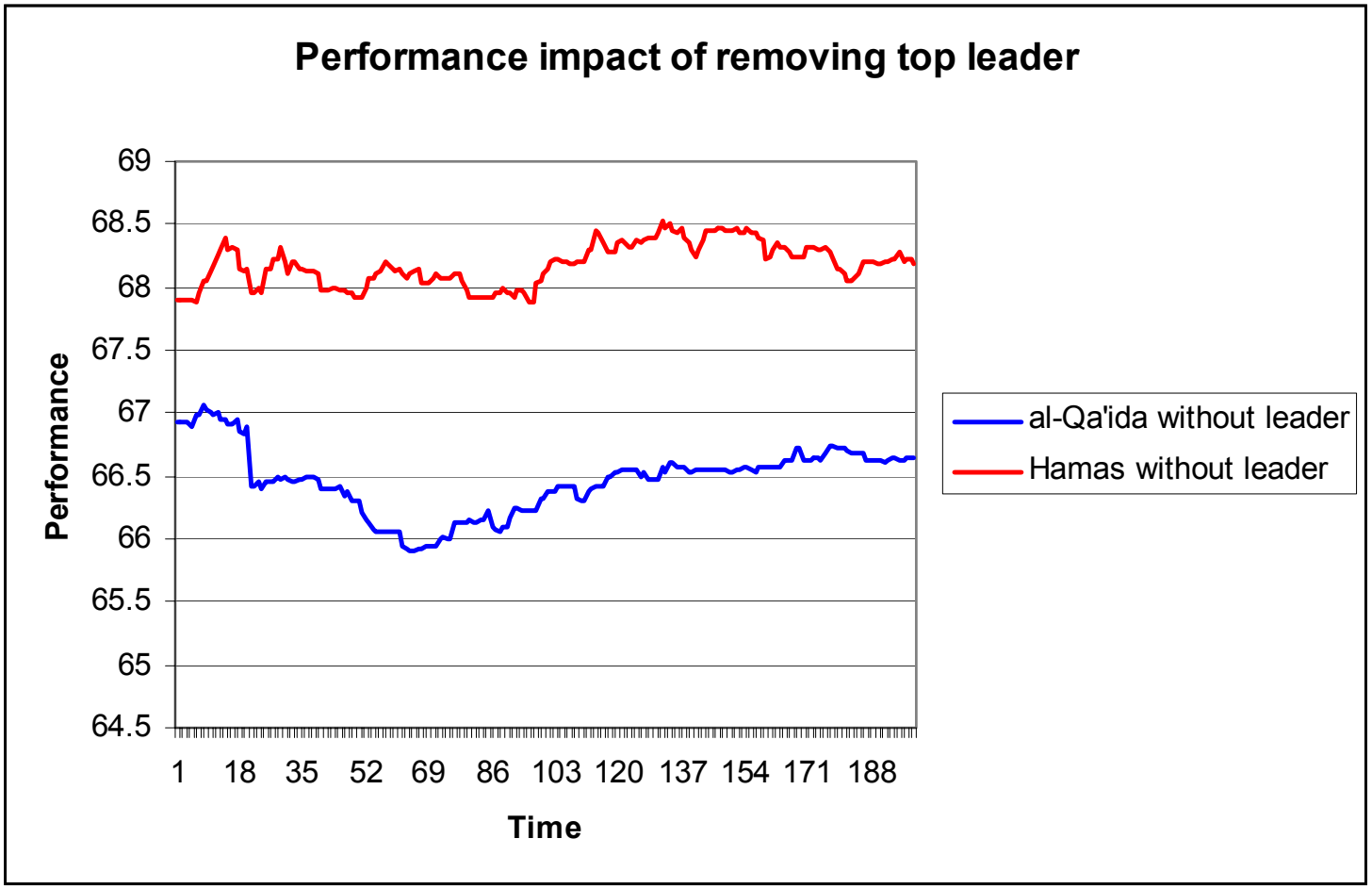




Before

After

Expected Performance After Removal of Top Leader



Range in Estimates

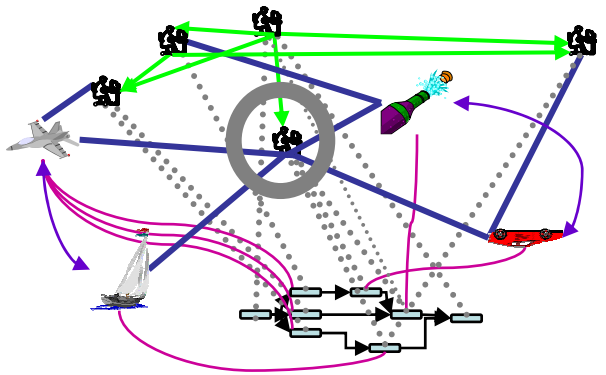
- **Hamas**
  - **Density**
    - **.03/.05**
  - **CD Yassin - .05/.04**
  - **Degree - 2**
- **Al-Qaeda**
  - **Density**
    - **. 02/.096 (.01 to .03)**
  - **CD bin Ladin - .05/.028**
  - **Degree 2**
- **Typical social network**
  - **Density**
    - **.3**
    - **Degree 7**

But – since the structure is apx consistent –
the results hold

Key Ideas of Dynamic Network Analysi

Meta-Matrix

	People	Knowledge	
People Relation	**Social Network** *Who knows who*	**Knowledge Network** *Who knows what*	**Assignment Network** *Who does what*
Knowledge Relation		**Information Network** *What informs what*	**Needs Network** *What knowledge is needed to do that task*
Tasks Relation			**Precedence Network** *Which tasks must be done before which*



Combine

Networks + multi-agent

Social science + computer science

Conceptual + network data

Emergent leaders – cognitive demand

Where Next

- Dynamic measures
- Visualizing dynamics
- Social “zooming” on the visuals
- Simulations – linking actions (beyond communication) and networks
- Explore personality additions
- Explore power added by using graph based pattern detection – like proximity

Related Work

- AutoMap – semi-auto extraction of network data from texts
- ORA –
- DyNet – evaluation of network dynamics and destabilization policies
- NetWatch – impact of data integration, sharing and control on ability to detect evolving network
- BioWar – city scale multi-agent network model of weaponized biological attacks
- OrgAhead – multi-agent network model of evolving organizational forms
- Construct – co-evolution of agent mental models and social networks
- ThreatFinder – social/knowledge management system for locating IP security risks
- Vista – estimating the evolving likelihood and impact of unanticipated events in urban settings