

Social Information Retrieval

Raymond D'Amore

703-983-1764 • rdamore@mitre.org

MITRE Sponsored Research

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

MITRE
Technology
Program

Problem

- The ebb and flow of information across the Web and within the enterprise allows us to speculate on the interests and alliances of all kinds of organizations. Who these groups are and how they align is of inherent interest since their collective behavior can shape local reaction and international opinion and can signal future threats and adverse action.
- The need is for technology that can monitor dynamic environments, detect community emergence, and track organizational behavior over time. This technology can potentially address problems that have international proportions (such as asymmetric threat), yet are also situated within the enterprise (detection of malicious insiders).

Background

The Web and corporate intranets represent a wide range of human interests and activities.

People and organizations leave evidence of their interests and affiliations through various aspects of their online behavior.

Communities typically emerge around common interests, and are linked together into networks dedicated to a particular cause or interest area.

Detecting important networks or communities, determining their purpose, and tracking changes has taken on significant importance.

“Networks are weapons systems”

MG Raduege, Information Operations Symposium,
San Diego, CA, Oct. 1999

The conflict over Kosovo has been characterized as the first war on the Internet. Government and non-government actors used the Net to disseminate information, spread propaganda, “attack” opponents, and solicit support for their positions.

Defense Science Board study on Transnational Threats
“The making of connections between otherwise meaningless bits of information is at the core of (transnational) threat analysis. Search methods current in use are not up to the challenge.”



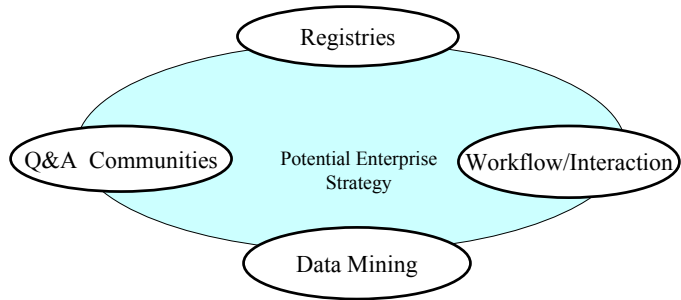
Objective

- Investigate new methods for detecting and tracking networked organizations, such as terrorists, activist groups, and communities-of-practice
- Detect potential vulnerabilities and predict potential new threats based on organizational structure and group synchronization or linkages
- Apply to key mission areas within the enterprise, and support sponsors in areas such as asymmetric threat, information operations, and indications and warning for homeland security

Activities

- **Problem-focused Research: Tracking Activist Groups, Communities-of-Practice in Scientific Domains, and Detecting Expertise Networks**
- **Core Technology Investigations:**
 - **Detecting Enterprise Community-of-Practice : detecting expertise networks, groups, and individuals spanning the formal and informal organization**
 - **Detecting Web Communities: preliminary work leveraging context-sensitive Web crawlers for locating emerging communities on the Web**
- **Prototypes and Models:**
 - **Expert Locator: expertise detection prototype**

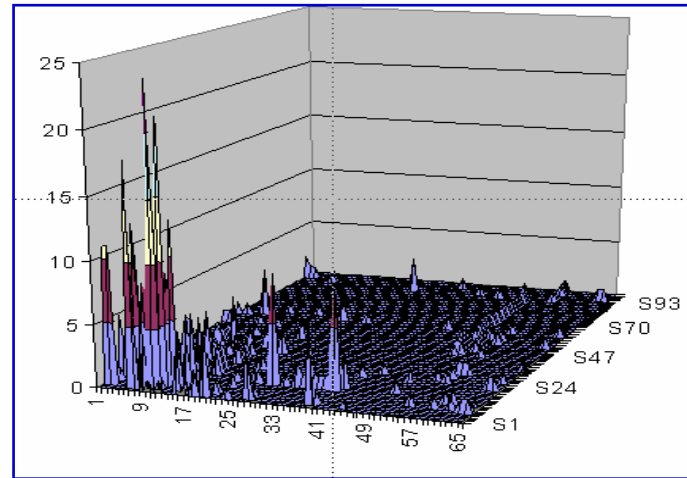
Highlight



- Heterogeneous search: integration of Enterprise Info Services with collected activity space behaviors
- Ecological model supports evidence aggregation: fusing evidence (actors, artifacts, activities, and the social network) into measures of expertise
- Sociometric DB supports dynamic community analysis

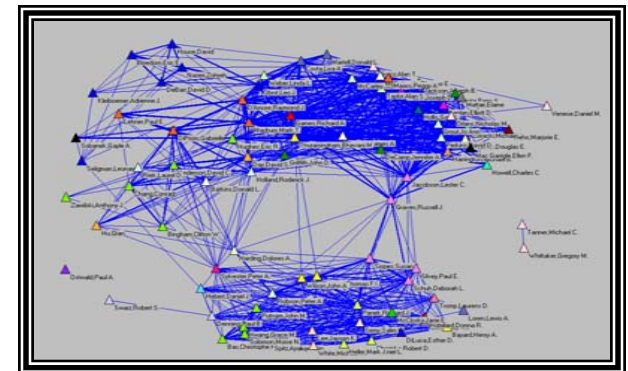
MITRE

Extracting Expertise from the Enterprise



**Query-based
Evidentiary-Social
Topology**

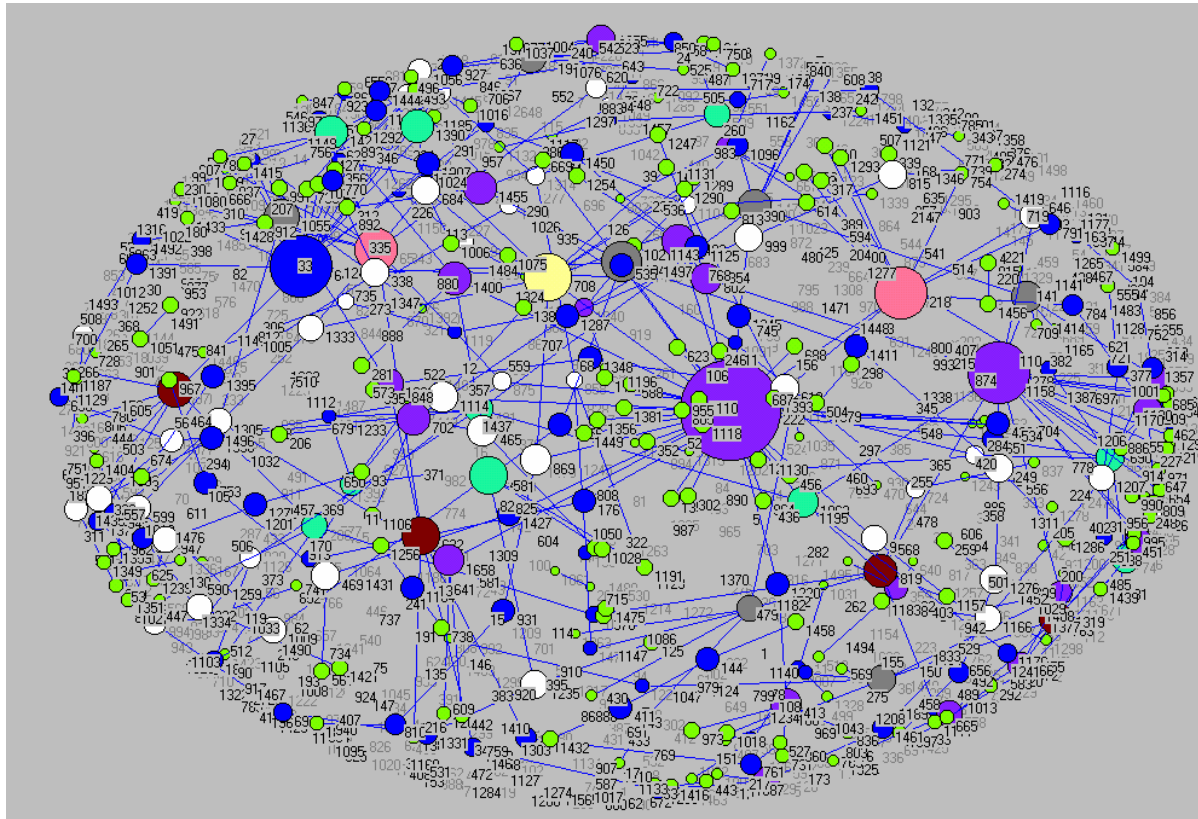
**Detected
Community of
Practice**



Impacts

- **Multi-disciplinary research ties together key concepts from information retrieval, social network analysis, and ecological community modeling**
- **Emerging capability to detect communities of practice or isolated areas of expertise across the virtual and physical enterprise. Evaluation underway**
- **Preliminary investigation of methods for detecting community networks on the Web**
- **Aligning research with key intelligence community problems; e.g., insider threat, asymmetric threat**

Future Plans



Near term: Detecting (Expertise) Communities

Long term: Dynamical Systems Modeling Applied to
Predicting Behavior of Temporal-spatial Community Networks