



# Knowing Terrorism

---

Nancy K. Hayden  
Advanced Concepts Group  
Sandia National Laboratories

January 2004



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. This document is SAND2004-0518P.





## The Need

---

There is nothing so likely to produce peace  
as to be well prepared to meet the enemy.

*General George Washington*

If everybody is thinking alike, then  
somebody isn't thinking.

*General George S. Patton, Jr.*

That general is skillful in attack whose  
opponent does not know what to defend; and  
he is skillful in defense whose opponent does  
not know what to attack.

*Sun Tzu*



# Formulating the Mess

---

## – Major Questions

- How do we wage a war against an ideologically driven social movement?
- What policies and actions comprise the strategic high road?
- What paradigm shifts are required to be effective?
- How do we ensure actions are guided by principles?

## – Principles

- Know the enemy, know oneself, know the whole system
- The whole is bigger than the sum of the parts
- Balance tensions: robust/secure; efficient/safe; episodic/normal
- Questions are to be explored, not resolved
- Success is the devil

## – Framework for Knowing

- Multi-minded, adaptive, self-organizing systems
- Characterized by unpredictable emergent behaviors

# The Complexity of Terrorism

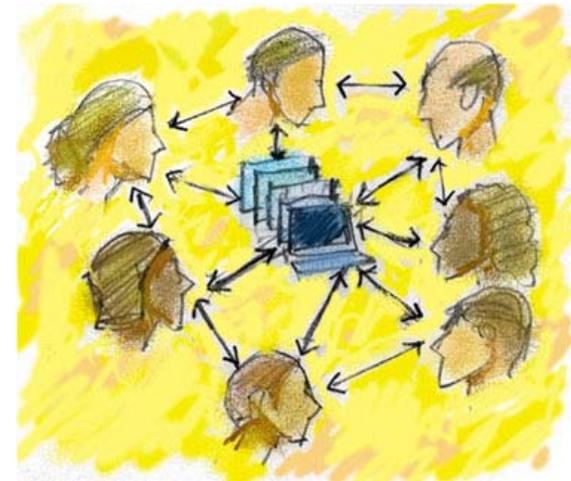
- **Diversity**
  - Adherents
  - Organizational structures
  - Contextual conditions
- **Adaptation**
  - Strategies
  - Methods and capabilities
  - Nonlinear interactions
- **Evolution & Co-Evolution**
  - Ideology
  - Networks
  - Sympathetic base of support



# The Approach: An Ecological Model of People and Technology

- **Knowing the Enemy**

- Diverse, distributed, collaborative network of experts and info
- Gaming based, scenario-driven data mining
- Simulation and analysis models for exploring behaviors and strategies



- **Multi-pronged action plan**

- Intelligence required to defeat enemies
- Military action to secure peace
- Civil/military cooperation for stabilization and reconstruction
- Private/public partnerships to foster economic development
- Advance in social institutions and values

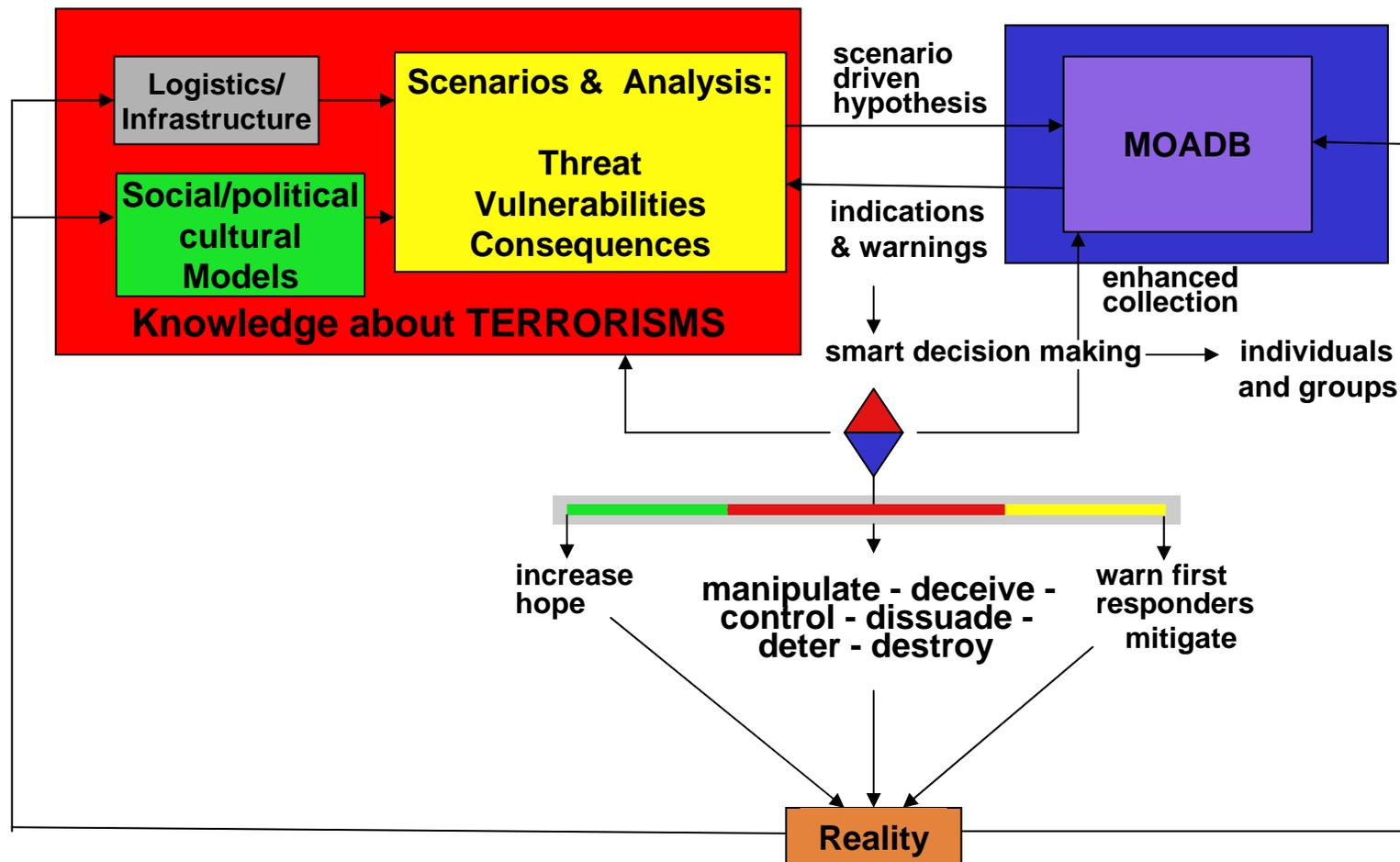
- Trust and good governance

- Mutual respect for human rights and capital development



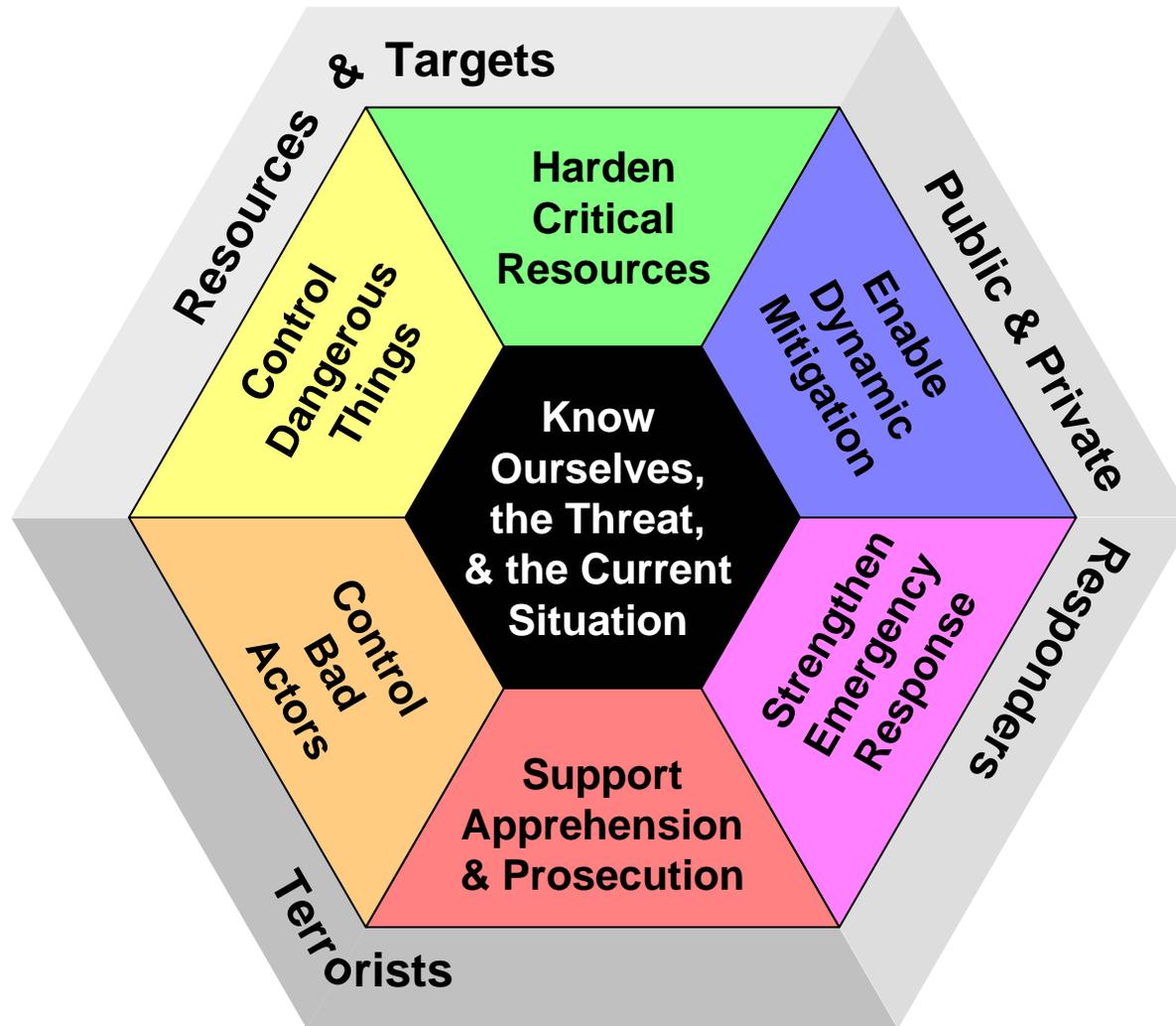
# Fighting Terrorism

*The key: understanding the complex system so as to shape the future*





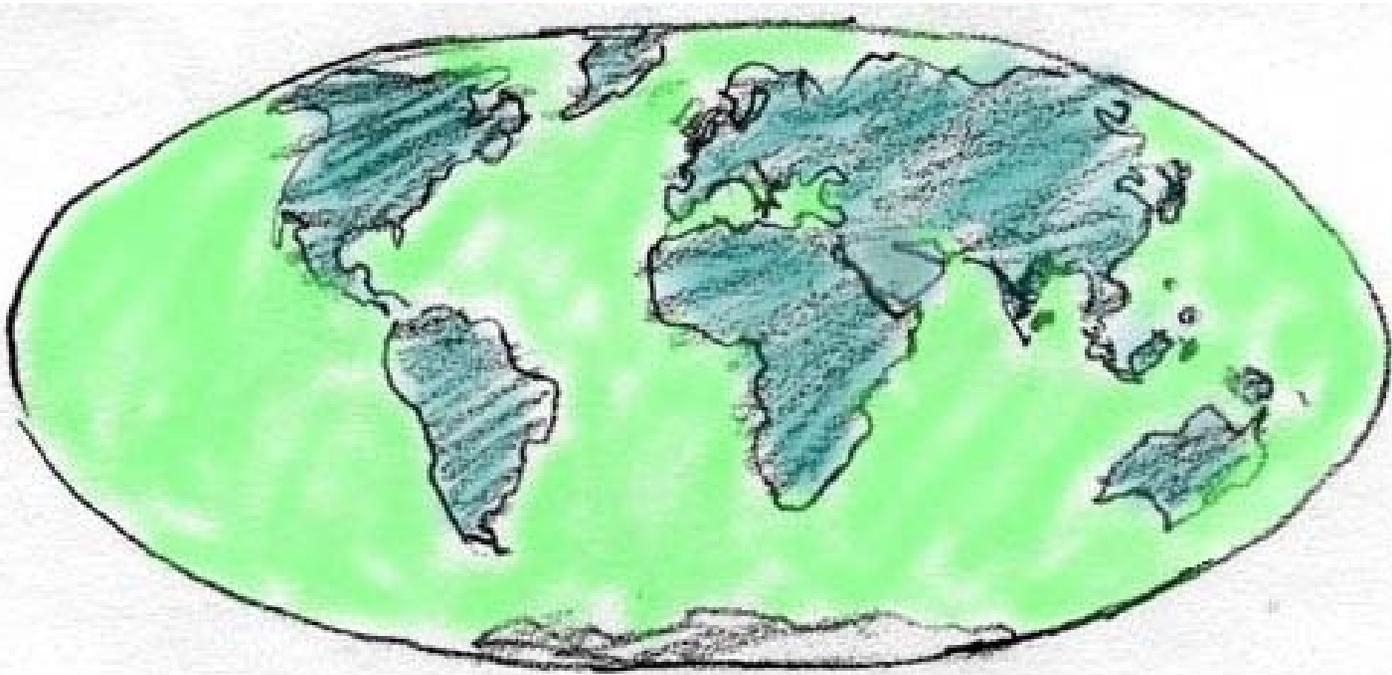
# Knowing: The Pervasive Underlying Need





# A Trip Around the World

---



***what really might be going on?***



# Afghanistan

“The situation in Afghanistan has been deteriorating. Increasing numbers of better-trained, better-equipped, and better-led Taliban cadres have stepped up their hit-and-run raids in order to demoralize the newly raised army and police of the Hamid Karzai government.”

Asia Times Online, 23 October 2003



*How do we anticipate the co-evolution of competing power/identity groups within the Arab and Islamic worlds?*



# Iraq

“The tipping point long anticipated by President George W. Bush may have finally been achieved Wednesday morning as thousands of jubilant Iraqis took to the streets to mark the beginning of the end of Saddam Hussein’s 24-year tyrannical rule of terror.”

LONDON, April 9 (UPI)

“War in Iraq has swollen the ranks of Al-Qaeda and galvanized its will by increasing radical passions among Muslims.  
The Guardian [United Kingdom], 16 October 2003.



*Tipping points: when are societal transition phases uni-directional and when are they bi-directional? What will our actions induce? What is the interplay of media coverage, public sentiments and reality?*



# India

---

The United States has designated as a terrorist Dawood Ibrahim, an Indian crime lord who has shared his smuggling routes with Al-Qaeda and funded attacks by Islamic extremists aimed at destabilizing the Indian government.

Press Release, U.S. Department of the Treasury, 16 October 2003.



*Where are key links in networks?*

*How robust are network operations to their removal?*

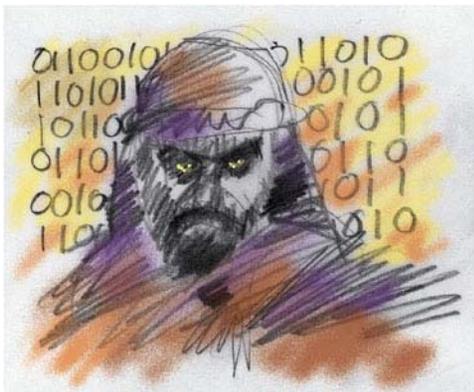
*Will new ones form in their place?*



# Iran

Saad bin Laden, one of Osama Bin Laden's oldest sons, has emerged in recent months as part of the upper echelon of the Al-Qaeda network managing the terrorist organization from Iran. Many experts believe this twenty-four-year-old had direct involvement in coordinating the 16 May suicide bombings in Casablanca.

Washington Post, 14 October 2003.



*How does a leader emerge?*

*How do we detect the imminent emergence?*



# Philippines

Philippine authorities backtracked over claims that a bioterrorism manual and traces of biological weapons had been found at a Jemaah Islamiyah terrorist hide-out. Examination of powders found at an apartment on the southern island of Mindanao showed they did not contain the tetanus bacteria as originally reported.

*Agence France Presse, 21 October 2003.*



***Co-evolution and perception: how does what I think about what you may be doing influence what I think and do and what you think and do in response to what I think and do?***



# Europe

The Iranian and Osama bin Laden terrorist networks, assets, and alliances built up in Bosnia-Herzegovina, Kosovo, Albania, Macedonia, Southern Serbia, and elsewhere in the Balkans are preparing for a significant new slate of operations.

*Defense and Foreign Affairs Daily, 15 October 2003.*



*How does one detect latent cells in networks, and anticipate their initiation triggers to create “giant stars”?*



# Yemen

Yemeni authorities have captured Khaled Abdul Nabi, chief of the Al-Qaeda-aligned Aden-Abyan Islamic Army. The group is believed to be linked to the suicide strike that crippled the USS Cole in Aden in 2000.

*Geostrategy-Direct, 21 October 2003*



*What dynamics control the synchronization of networks, creation of “small worlds”, and how can these dynamics be pre-empted or broken?*

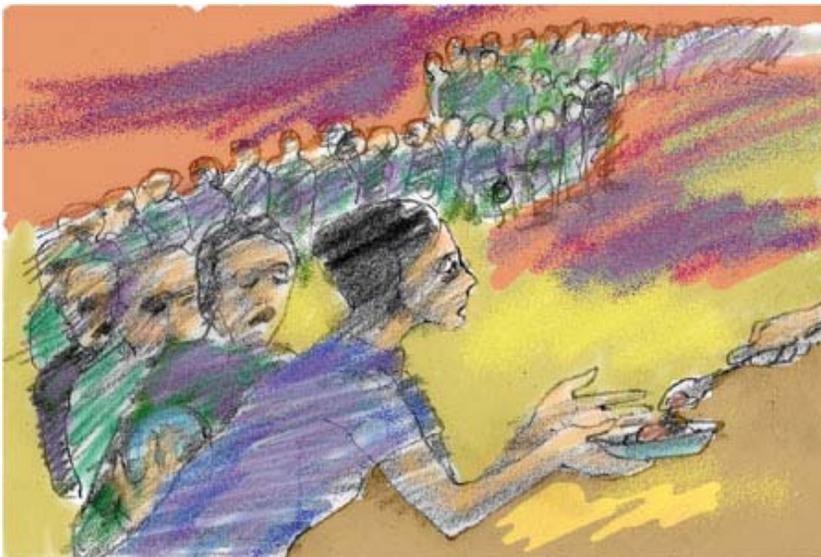


# USA

The FDA has issued a risk assessment for food terrorism and other food safety concerns.

Food and Drug Administration, Department of Health and Human Services, 7 October 2003, Notice in the Federal Register (Vol.68, No. 197, 10

October 2003



*What are operational dynamics between interconnected networks: military, political, economic, social, critical infrastructures?*

*Is there really a threat?*

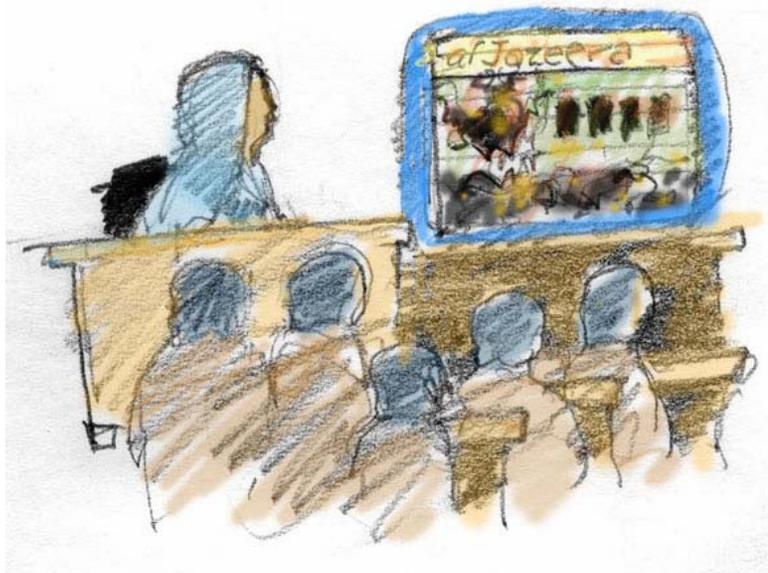


# The World

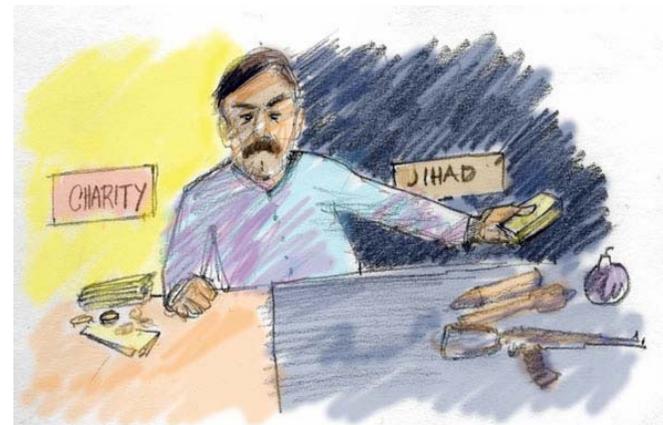
## Terrorism Inc.

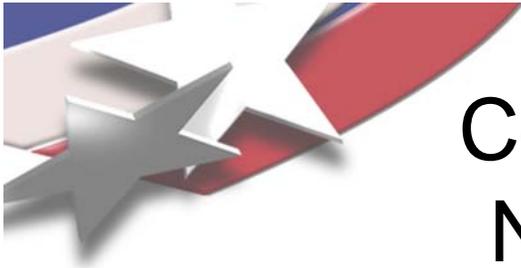
### **Al Qaeda Franchises Brand of Violence to Groups Across World**

Leaders of the al Qaeda terrorist network have franchised their organization's brand of synchronized, devastating violence to homegrown terrorist groups across the world, posing a formidable new challenge to counterterrorism forces, according to intelligence analysts and experts in the United States, Europe and the Arab world.



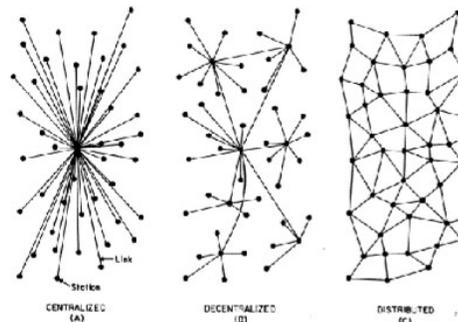
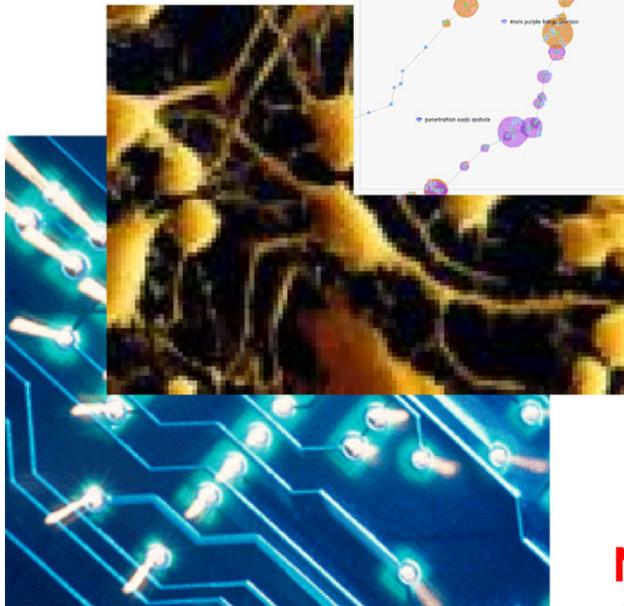
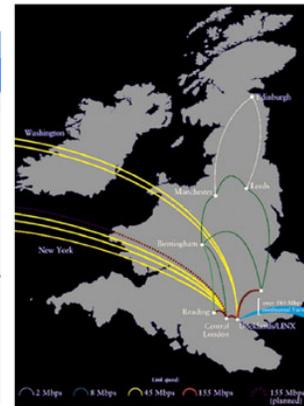
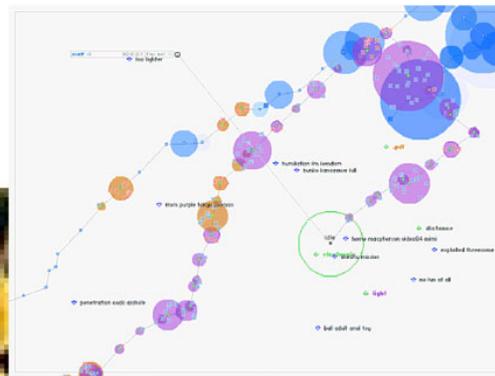
Washington Post Friday, November 21, 2003





# Complexity Science Offers New Analysis Paradigms

## Agent Based Modeling web games



## Network Analysis CASOS at CMU

## SFI Workshop April 10-11, 2003

How Complex Adaptive Systems Dynamics are Related to Understanding and Modeling Terrorist Behavior

*Sandia, Argonne, LANL, CIA, DTRA, MITRE, Navy, Cornell, U of Penn, Intel, CMU, Icosystems, USAF, Galisteo, Humana, Alidade, U of Maryland, MIIS, Brookings, NYU*



# Knowing About Complex Systems is Hard

Murray Gell-Mann, Nobel Laureate, Santa Fe Institute, as quoted by Thomas Friedman in “The Lexus and the Olive Tree”

**“When dealing with any nonlinear system, especially a complex one, you can’t just think in terms of parts or aspects and add things up and say that the behavior of this and the behavior of that, added together, makes the whole thing.**

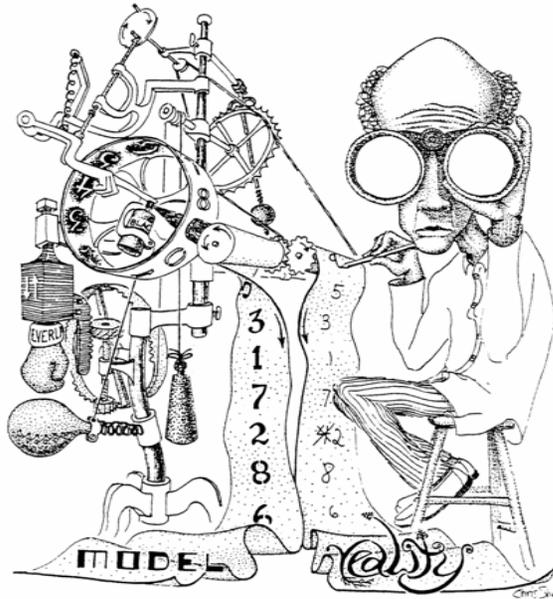
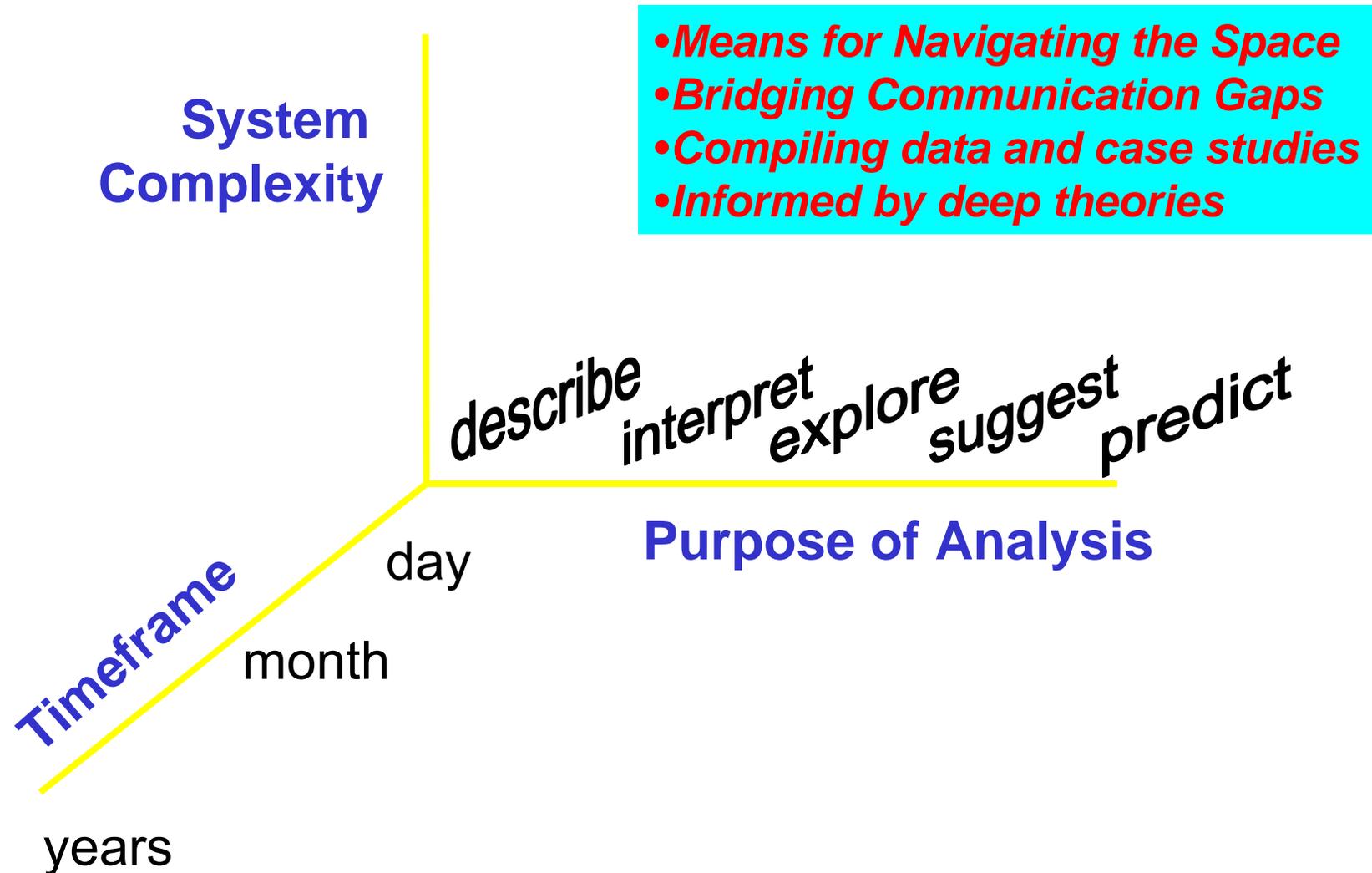


Fig. 50 - The two data streams.

**With a complex nonlinear system, you have to break it into pieces and then study each aspect, and then study the very strong interaction between them all. Only then can you describe the whole system.”**



# Parsing the Problem





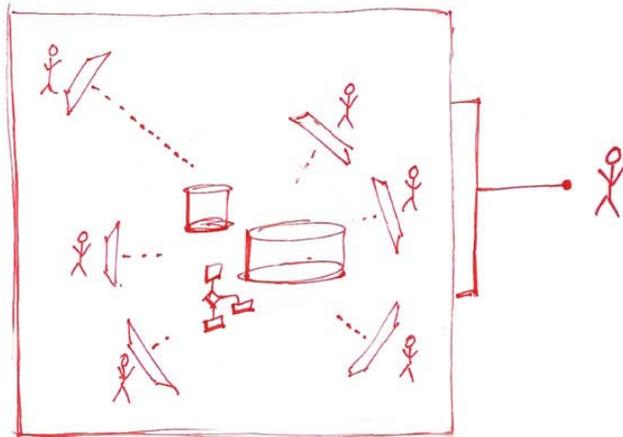
# KnowNet Concept

## January - August 2003

Distributed, emergent collaborative **experts** network across disciplinary, ideological, and cultural boundaries

Accumulate real information in real system so real people can see whole picture to interdict/prevent terrorism

Virtual “mind of the fox” at interstices between USG, foreign experts, academia, and private research institutes



**KNOW NET**

- Deep domain knowledge assembled on demand
- Relevant knowledge discovered across multiple domains and venues
- Ready access to analysis tools
- Knowledge cumulatively maintained in open, controlled environment



# Homeland Security Collaborations

---

- **Building Community and Information Integration**

- **FBI:** Joint Terrorism Task Forces, **COPLINK**
- Intelligence Community: **TTIC**, internal systems
- **DHS:** policy studies, geographically based vulnerabilities

**Unmet Needs:** *bridges within and between compartments, domain experts, units; resolve security and culture concerns*

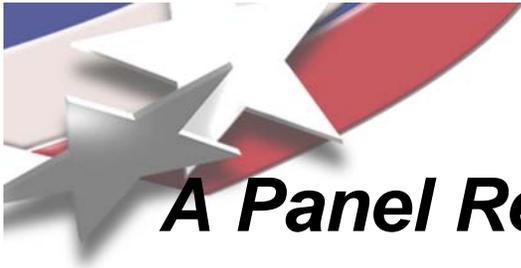
- **Open Source Analysis**

- **DIA** “experiments”
- **University, MIIS, RAND** data bases and analysis
- **MIPT**

**Unmet Needs:** *expanded community (especially international), analysis and collaboration tools; problem focus; diverse forum*

- **Policy Analysis**

- Center for the Study of the Presidency



# ***A Panel Report to the President and Congress:***

---

## **Comprehensive Strategic Reform**

*Center for the Study of the Presidency September 2001*

- New U.S. national security consensus and decision-making structures are required
  - Dynamic, fluid, continuous, trusted, comprehensive
  - Incorporates the “edges” on equal basis with “hubs”
  - Capabilities and intent based
- Integrated and agile U.S. strategy must leverage more than military power
- Agility, not rigidity, is needed as a mindset



# National Science Foundation Blue Ribbon Panel 2003

---

## •Vision

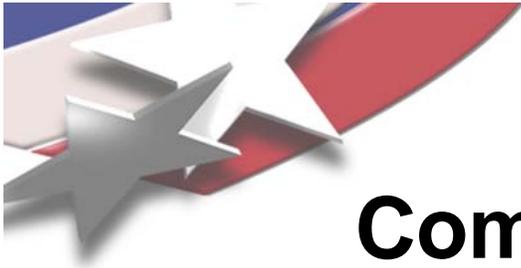
- Use cyber infrastructure to build more ubiquitous, comprehensive digital environments that become interactive and functionally complete for research communities in terms of people, data, information, tools, and instruments and that operate at unprecedented levels of computational, storage, and data transfer capacity.”
- interagency and international in scope

## • Spending

- an additional \$1 billion per year to support scientific research

## • Risks of failing to do so:

- **lack of coordination, which could leave key data in irreconcilable formats;**
- **long-term failures to archive and curate data collected at great expense;**
- **artificial barriers between disciplines built from incompatible tools and structures.**



# Common Theme Many Names

---

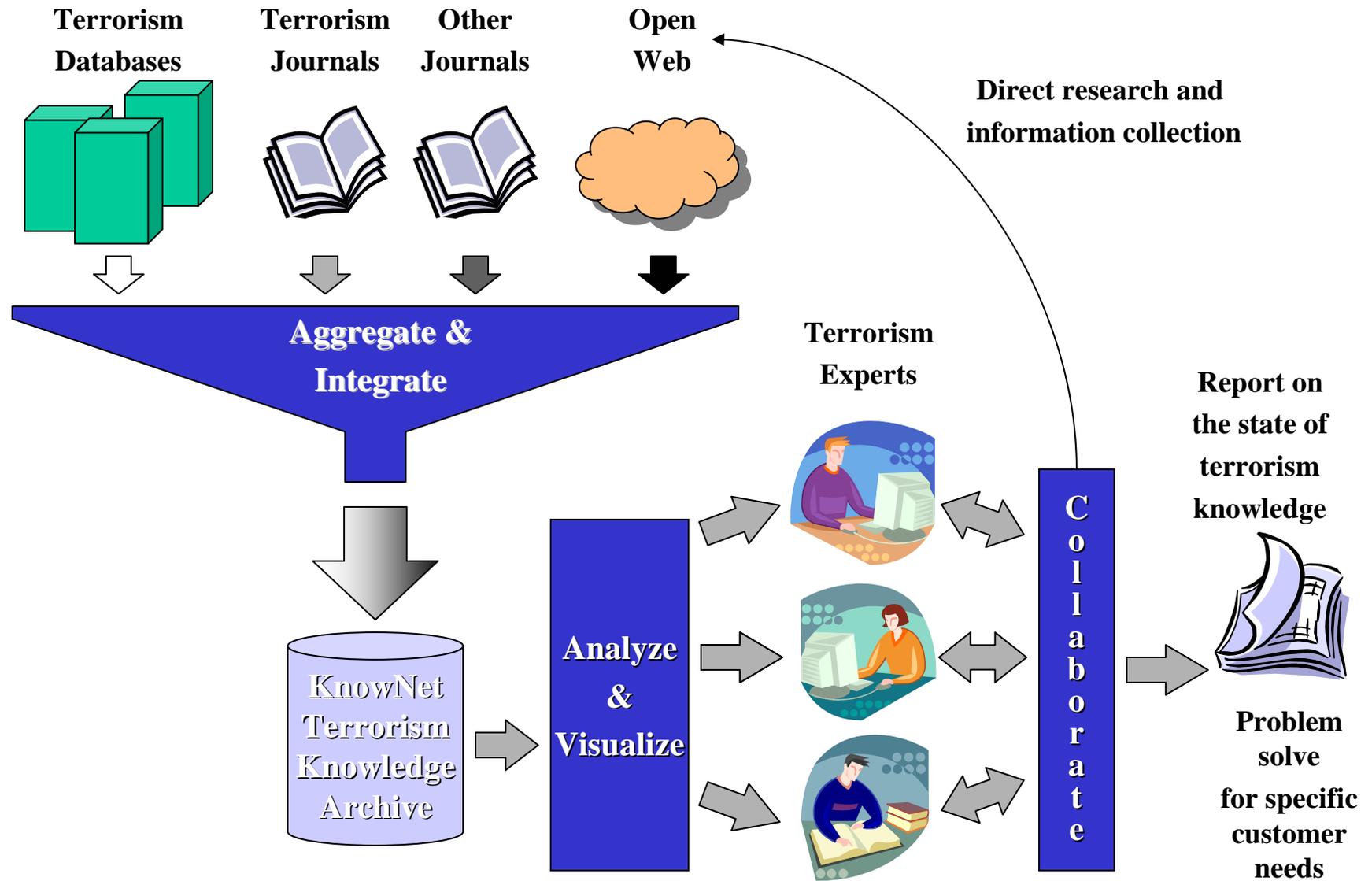
- “A **COLLABORATORY** is a network-based facility and organizational entity that spans distance, supports rich and recurring human interaction oriented to a common research area, fosters contact between researchers who are both known and unknown to each other, and provides access to data sources, artifacts and tools required to accomplish research tasks”

*Science of Collaboratories Alliance*

- *Grid community, network, co-laboratory, virtual community, community of practice, virtual science community, e-science community,*

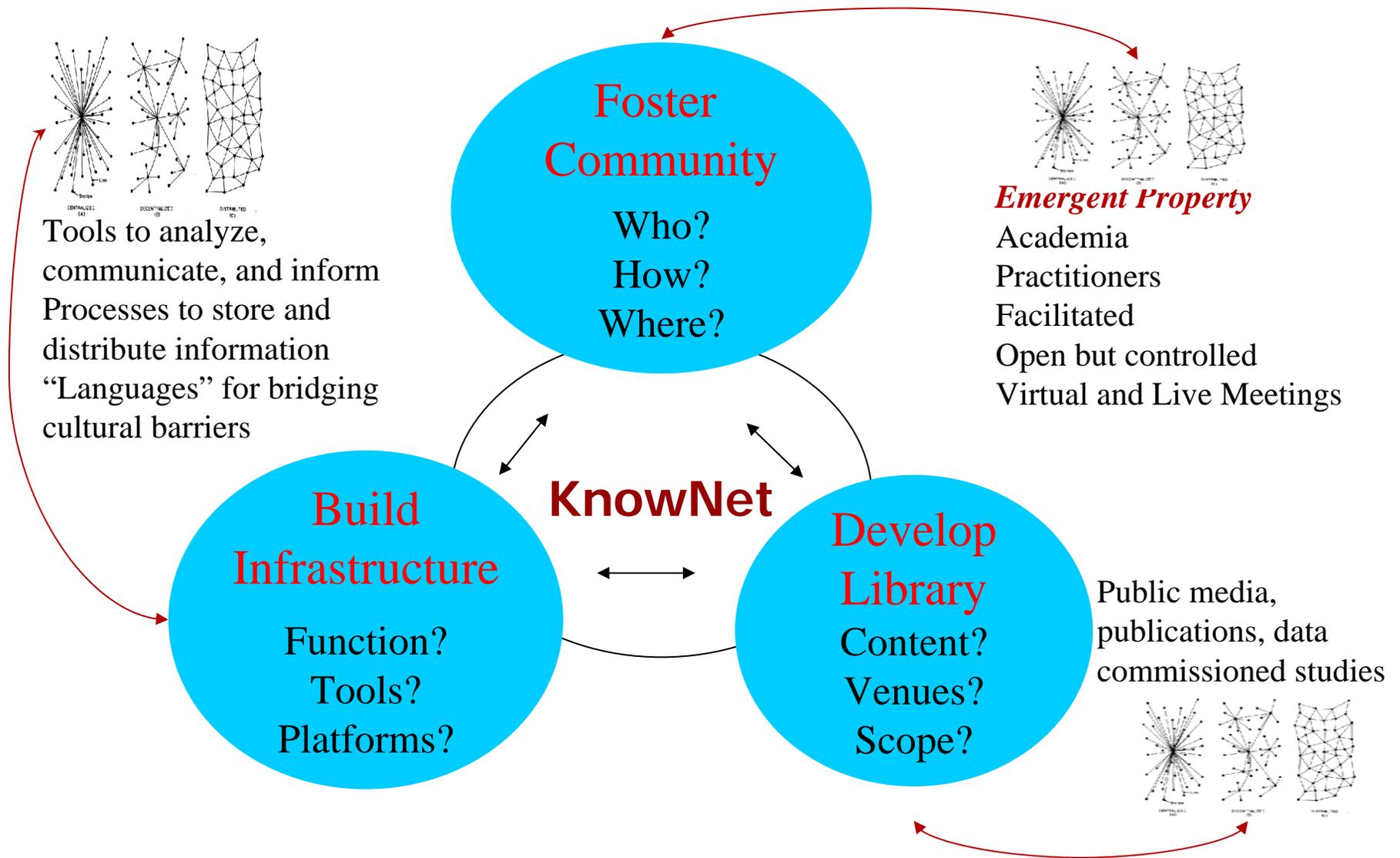


# The Approach





# What is Involved?



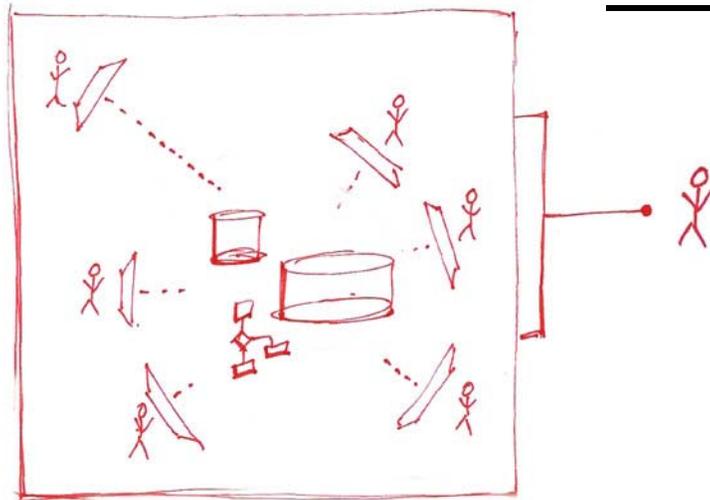


# KnowNet Concept

Distributed, emergent collaborative experts network  
across disciplinary, ideological, and cultural boundaries

Accumulate real information in real system so real people  
can see whole picture to interdict/prevent terrorism

## Bottom Line



**KNOW NET**

We need adaptive, user driven,  
JIT access to self-organizing  
system of knowledge for  
cross-sector evaluation of

- Threat assessments,
- Research agendas,
- Responder actions,
- Policy options, and
- Strategic planning



# KnowFest

---

- ACG-sponsored workshop August 2003 vetting the KnowNet concept with diverse experts
- Questions addressed:
  - what needs KnowNet would serve
  - what else exists and is need being met already
  - how the network might be employed by various end users and researchers,
  - how the human and technical aspects of the network might be structured,
  - how the KnowNet might be grown and managed,
  - how it might be funded



# KnowFest Attendees

---

- Gary Ackerman, MIIS
- Harry Betz, FBI / NM AG
- Jeff Cares, Alidade
- Hsinchun Chen, U of AZ
- John Cummings, DHS
- David Hamon, DTRA
- Merle Lefkoff, LANL
- Mark Maybury, MITRE
- Ariel Merari,
- Patricia Medvick, PNNL
- Jerrold Post, GWU
- Raghu Ramakrishnan, U of WI
- Marc Sageman, U of PA
- Desmond Saunders-Newton, DARPA
- Marissa Urgo, DOE
- Rick Craft, Sandia
- Patricia Gingrich, Sandia
- Joe Harris, Sandia
- Nancy Hayden, Sandia
- Dwight Miller, Sandia
- Elaine Raybourn, Sandia
- Gordon Smith, Sandia
- Ken Washington, Sandia
- Gerry Yonas, Sandia



# Common Vision Developed at KnowFest

---

- Emergent community of diverse experts and users
- Self-organizing state of the art communication
- Facilitated, state of the art collaboration tools
- Access to, and supported use of, sophisticated data analysis, visualization, and modeling tools
- Content
  - Relevant, accessible, cross-sector, multidisciplinary, multi-format, evolutionary
  - State of the art knowledge exploration and discovery
- Provide different views according to the need



# KnowFest Key Findings

---

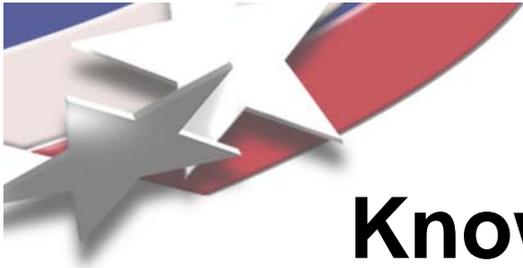
1. Need is Real
  - We don't know what we know about terrorism
  - Entities who *could* make use of what is known, don't
  - People who assess threat from hard science perspective think differently than social sciences and vice versa - different perspectives are important
2. Need is not being met as envisioned
  - Much can be gained by creating an open community across institutional, disciplinary, and geopolitical boundaries that integrates with analysis capabilities
3. Much can be done in very short order building on existing initiatives with existing tools
4. Full capabilities requires solving technical, social, and institutional barriers



## What IS in Place

---

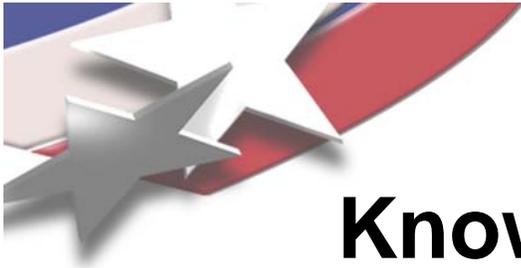
- Intra-institution collaboration spaces
  - Institutional control provides for security
  - Cross-compartment and institution collaboration difficult
- Inter-institution collaborations
  - Varied successes under study by NSF [Collaboratories](#)
- Publicly accessible on-line venues
  - On-line discussion and information sharing forums
    - [Terror and Technology On-Line Conference](#)
  - On-line information consolidation and reporting
    - [The Terrorism Portal](#)
    - [Southeast Asia Terrorism Portal](#)



## KnowNet Use Cases: Example

---

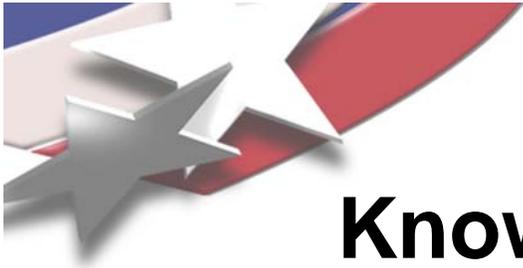
- Provide regular update of trends and changes in the social network and characteristics of active terrorist cells
  - Track geographic density and intensity of activities
  - Track demographic trends of participants
  - Perform comparative systems analysis across primary social, psychological, technical parameters
  - Generate updated profiles based on customer defined characteristics and metrics
- Community Involved: open source data base holders in multiple countries (e.g., US, Israel, UK, Singapore, France, Germany) maintained by academia, think tanks, and national labs



## KnowNet Use Cases: Example

---

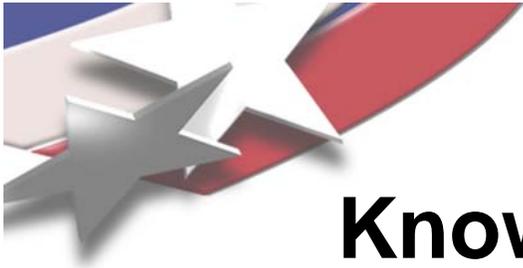
- Facilitate collaborations for high quality analysis
  - Bring together social scientists and information technologists
  - Exploit computational resources and expertise in national labs for data visualization and modeling
  - Provide archival repository for analyses accessible to future researchers
  - Provide format and forum for presenting and discussing results of analyses among experts
- Community involved: academia, think tanks, national labs, federal agencies



## KnowNet Use Cases: Example

---

- Evaluate “design basis” threat scenarios for developing strategies for defense and response
  - Engage diverse community of experts in analysis of likelihood and credibility of scenarios
  - Provide open but controlled-access forum for dialogue, debate, and documentation of experts’ views
  - Provide venue for periodic and episodic review and updates of evaluations
- Community involved: academia and think tanks (with select international participation as appropriate), federal entities, national labs



## KnowNet Use Cases: Example

---

- Convene virtual panels of diverse experts on complex policy issues
  - Provide network of knowledgeable experts
  - Provide platform for virtual meetings
  - Provide common background information sources for consideration
  - Provide ongoing discussion space during period of examination of issues
- Community involved: academia, think tanks, federal agencies



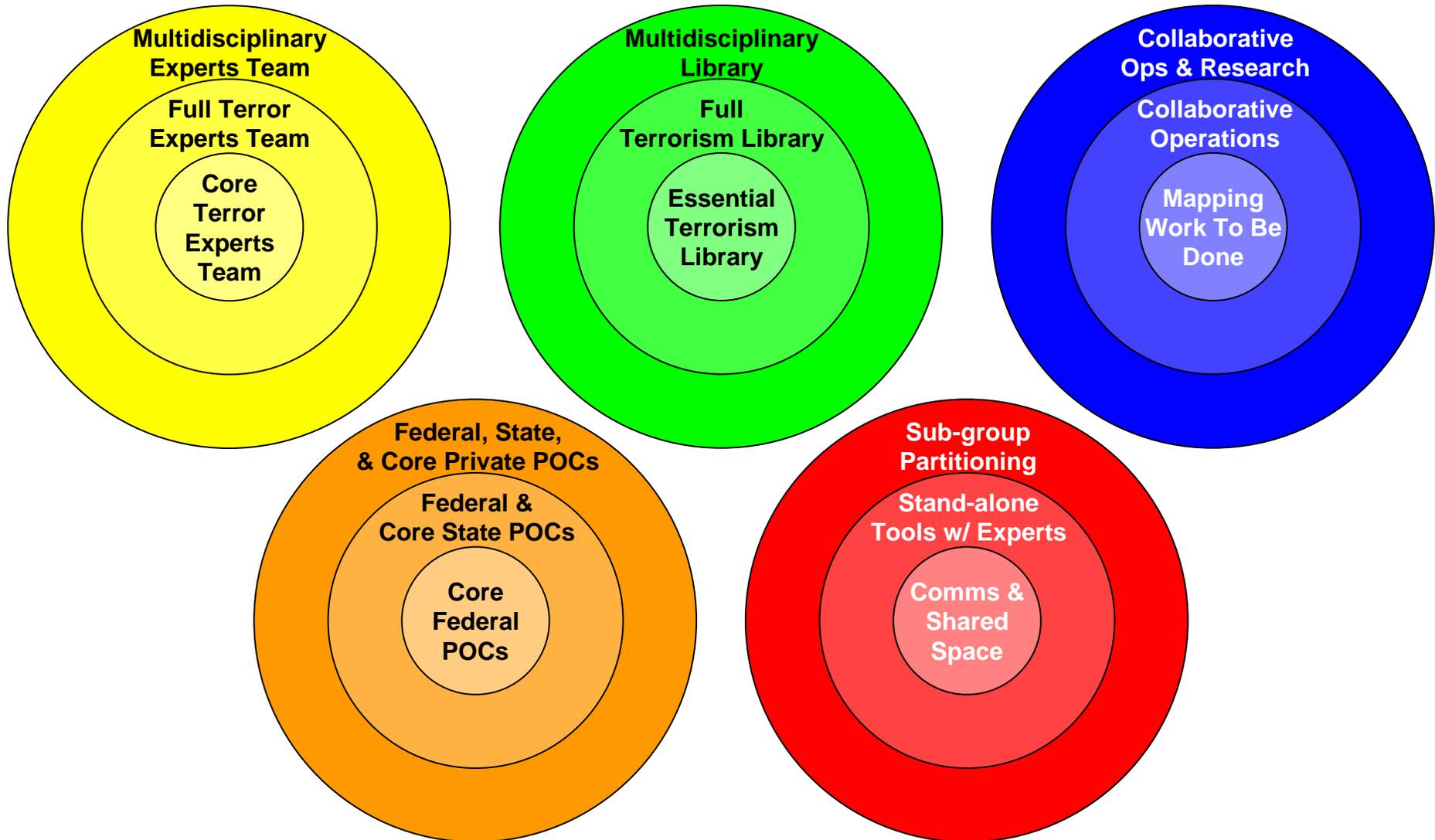
---

## What Might this look like?

Mock-Up from KnowFest provides  
enduring architectural vision



# Network Evolution





# KnowNet Community Profile

	Domain expertise	Information Technology	Knowledge management	Security Policy and Issues
Think Tanks	X			X
Academia	X	X	X	
Fed, state, local government	X		X	X
National Labs, FFRDCs		X	X	X
Private	X	X	X	



# Information Architecture

---

Home

Members

Toolbox

Library

News

Collaborative Work

- Global Navigation
  - Home (orient the user with dynamic, compelling content)
  - Members (social network)
  - Toolbox (research tools)
  - Library (local documents, external sources)
  - News (KnowNet internal, external summaries)
  - Work Together (workplace, meeting space)
- Local navigation within global categories



# Members

Home

**Members**

Toolbox

Library

News

Collaborative Work

- Build community and find expertise
  - Searchable profiles
  - Contact Information
  - Presence: Who's online
  - Relationships
- ContactMap (Nardi, Whittaker, et al. ATT Research)
  - Interactive social network application
- April 2002 **Communications of the ACM**, Volume 45 Issue 4





# Knownet Toolbox

Home

Members

Toolbox

Library

News

Collaborative Work

- Provide information visualization and analysis tools
  - VxInsight
  - Attensity (syntactic and semantic freeform text analysis, discovers entities and relationships)
- Access to scenarios and models



QPtools edit

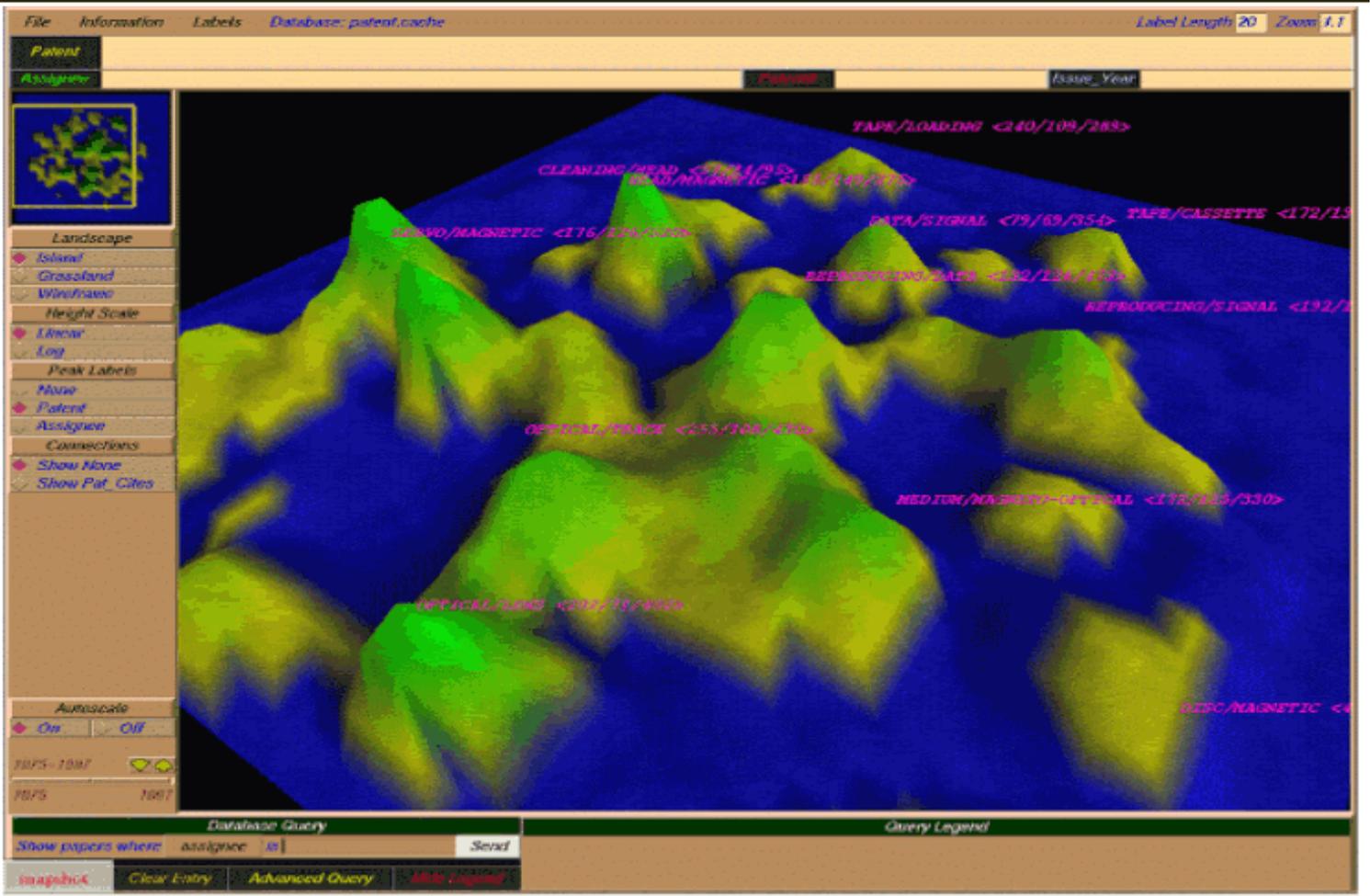
Network models

3d models

Scenarios

Visualizations

VxInsight





# Library

Home

Members

Toolbox

Library

News

Collaborative Work

- Access to internal and external information sources to aid researchers and feed the toolbox
- Member defined collections
  - data sets
  - semantic analysis results
  - landscape and other topographic analyses
- Bibliographic summaries
- Community member critiques and links
- Federated search
- Searchable, indexed collections (e.g., Jane's)



# News

---

Home

Members

Toolbox

Library

News

Collaborative Work

- Provide internal and external news
- Custom searches of predefined categories
- Foreign Language translation
- Internal: community message board, alerts



# Working Together

Home

Members

Toolbox

Library

News

Collaborative Work

- Enable communication and collaboration
  - Multiple modes for information transmission
  - Infrastructure for interactive problem solving and concept exploration
- Facilitate the formation of specialized groups within the community
- Provide a secure data repository/file sharing forum
- Secure and non-secure environments



---

**WHERE ARE WE?**



# Creating a Trusted Network for Homeland Security

---

## Markle Foundation Reports calls for SHAREing

- **Public/Private Data Debate : October 2002**
  - Most of the real frontlines of homeland security are outside of Washington DC
  - The government needs access to public and private sector data
  - The DHS should develop innovative service delivery models for information held within and outside USG
- **Need for System-wide Homeland Analysis and Resource Exchange: December 2003**
  - Government is a long way from creating the dynamic, distributed network for sharing and analysis envisioned
  - Network requires people, processes, and information developed hand-in-hand with technology and “rules of engagement”
  - Technical architecture should optimize abilities of all players

[Reports](#)



# Making KnowNet real

---

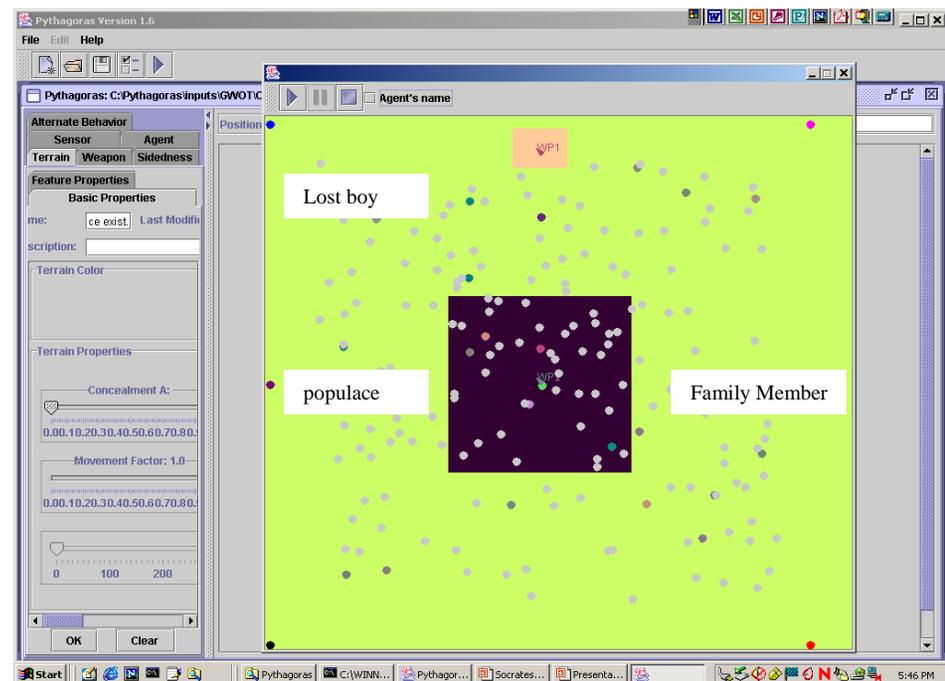
- Maintain Initial KnowFest community
  - Uploaded community list to existing MITRE Portal
  - Collaborations initiated among participants
  - Created an access controlled website for prototyping features and capabilities
- Transition KnowNet nucleus to CSP
  - Online database and knowledge-management capability to support senior homeland security analysts and policymakers.
- Support research for additional capabilities
  - Enhance informatics infrastructure and community
  - Address Markle Foundation findings



# Collaborations Initiated

- Agent Based Model of Terror Cell Formation
  - SNL, Project Albert, U of Penn, CAA
- Public response to Terror
  - U of Az, U of Penn, Private consultant
- Al Qaeda Network Analysis
  - U of Penn, U of Az, SNL, PNNL
- Data Base Integration
  - pending

## Pythagoras



# Collaboration: Social Scientists and Software Specialists

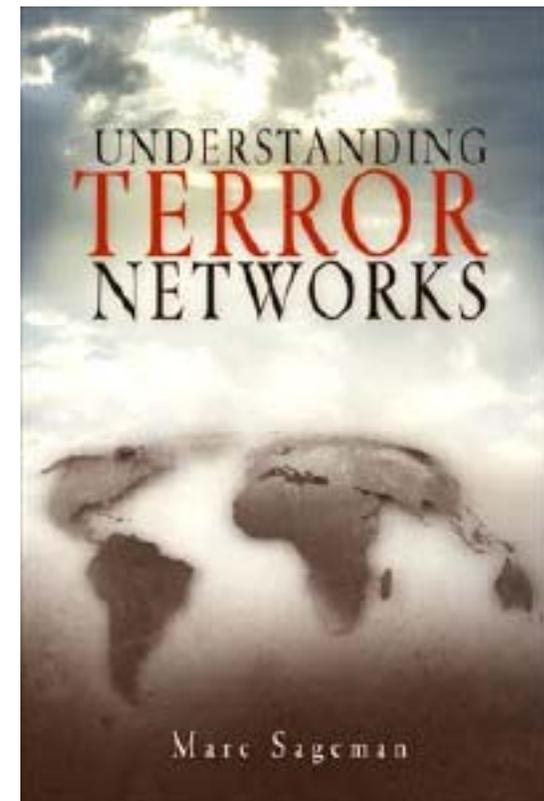
- **Participants**

- *Dr. Marc Sageman (U of Penn)*
- *Dr. Hinshen Chen (U of Az)*
- *Nabeel Rahal (SNL, PNL)*

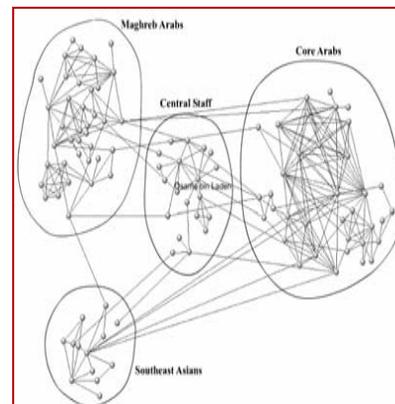
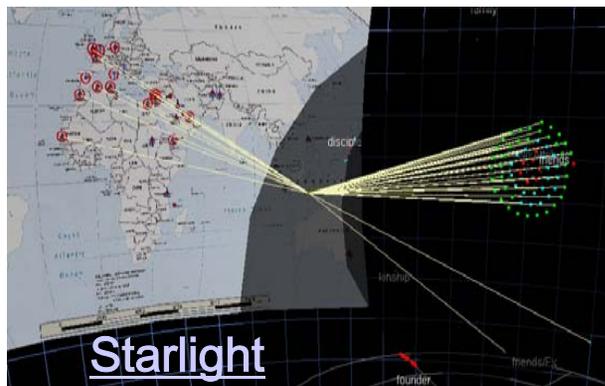
- **Impact**

- *Network analysis allowed exploration of scientific hypothesis and new understanding of cell formations*

## Understanding Terror Networks



## U of Az





# Prototyping Features: Noternet

The screenshot shows the KnowNet Anti-Terrorist Community of Practice website. At the top right, there are links for "My Places" and "Home". Below the header, the user "Nancy Kay Hayden" is logged in, with a "Sign Out" link. A navigation bar contains buttons for "New...", "Edit", and "Check Out...", along with icons for a folder, a document, and a trash can. A "Contents" sidebar on the left lists: KnowNet Home, Community Room, Hot Topics for Discussion, Public Media & News Room, Analysis Tools, Libraries & Collaboration..., Using This System, Report Problems, and Index. The main content area features a "Quick Links for Direct Access!" section with links: "You Evaluate KnowNet", "Access E-Mail Archives", "On-Line How To Use KnowNet", "Report Problem with KnowNet", "Who is in KnowNet?", "KnowNet Structure", "Add Your Bio", "View KnowNet Structure Map", and "Suggest KnowNet Improvement". Some links are marked with "NEW" icons. Below the quick links is a "Welcome to KnowNet" message: "You have joined a community of individuals from diverse areas of expertise working together to deepen our understanding of the phenomenon of terrorism and the threat it poses to the national and international security. This place is yours; a tool to help you work with others of like interest to create a trusted community and body of information. This implementation is a prototype based on concepts originally vetted at the KnowFest. As a prototype, it will be changed as you determine it needs to be."

- **Searchable Repository**  
*databases, publications, media reports, etc*
- **Collaboration Support**
- **Analysis Tools**



## KnowNet at CSP

---

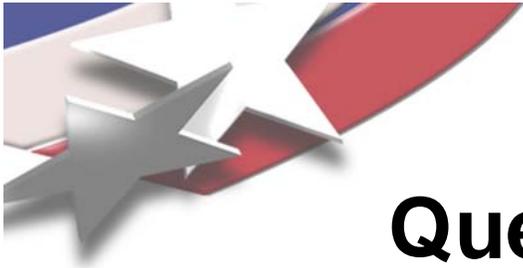
- Support the Existing Project Goals:
  - Gather in one place key executive summaries and recommendations
  - Provide access to fully searchable reports, documents, Executive Branch policies and strategies and Congressional testimony;
  - Identify gaps in research and policy.
- Provide platform to expand capabilities and resources
  - outreach mechanism through KnowNet community
  - additional database population
  - tool for senior Homeland Security analysts, policymakers, state and local officials also will have access
- Supplement with research results
  - Leverage existing information technology research results
  - Support with results of future findings and developments



# What's In Place

---

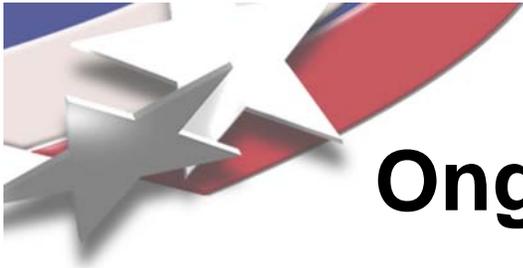
- Community
  - Academic researchers, government officials, law enforcement, information technologists, analysts
- Architecture
  - Community rooms, library, collaboration spaces
- Content
  - ACG & Sandia research: extensive bibliographies, presentations, studies
  - KnowFest Participants' individual contributions
  - Publicly accessible information
- Information Infrastructure



## Questions for CSP/KnowNet

---

- What is likelihood and credibility of DHS design basis threats?
- What strategies in Iraq will engage the public in suppressing terrorist activities there?
- What role does media play in the war on terror?
- How can US security policy reduce terror in the public?



# Ongoing Research Initiatives

---

- NSF
  - Science of Collaboratories
  - Partnerships for Advanced Computing Infrastructure
  - Pittsburgh Terascale Computing System
  - Information Technology Research Initiative
- DOE
  - National Collaboratories Program
  - Scientific Discovery through Advanced Computing
- NIH
  - Biomedical Informatics Research Network
- DHS, DOD, Intelligence



# Applied Research Goals

---

1. Architect and build an adaptive informatics infrastructure.
2. Define and build proof-of-concept capabilities that demonstrate the value of an informatics infrastructure in increasing collaboration and coordination across disciplines.
3. Demonstrate the power of an adaptive infrastructure as opportunities arise to support DHS counterterrorism efforts and to integrate with external projects without requiring adoption of KnowNet schema
4. Develop and execute a plan for community outreach that includes demonstrations of significant new capabilities to attract participation and continued support.
5. Evaluate and document the success of the project in terms of community interest and support, technical capabilities, etc. and recommend a continuation path to key stakeholders.



## Key Research Needs

---

- Insert from SOC, NSF and Markle report
- Validate with SNL/8900/8300 and user community



# Summary

---

- We came, we saw, we brainstormed, we developed our idea, we nucleated it, we transferred the embryo and are continuing to make better.