Computational Social Science, Culture and the Global War on Terror

Rebecca Goolsby, Ph.D.
Code 342, Office of Naval Research
goolsbr@onr.navy.mil
(703) 588-0558

Asymmetric Threats Before 2000

The breakup of the Soviet Union significantly changed the nature of threats to U.S. national security. U.S. intelligence and military strategists identified “asymmetric threats” as a growing and significant danger beginning in the early 1990s .

In the early 1990s, terrorist organizations were characterized as small in size with limitations of resources, personnel and knowledge base. Virtually all of these were focused on achieving local or regional goals.

<u>State sponsorship of violent groups was the chief concern of military and intelligence communities.</u>

From Threat Groups to Threat Networks

U.S. pressures on nation states to end sponsorship of terrorist organizations initially caused problems for these groups. However, they were able to adapt.

- Movement of headquarters and dispersion of people and assets across many states transformed local groups into regional, transnational organizations
- Social ties between groups were established and became increasingly important.
- Cooperation between groups began to coalesce into a network organization.

osama bin laden

Taking Out the Leadership Doesn't Stop Terrorism By Itself

- JI, an Al Qaeda subnet, captured most leaders after the Bali Bombing
- Ji was STILL able to function as a terrorist organization
- This is due to NETWORK HEALING
- **Marriot Bombing demonstrates that focusing on disconnecting the leadership is not necessarily the best strategy**

Islamist Terror Networks Evolving

MARCH 11, 2004 MADRID

THE NEXT GENERATION

Like minded, militant indigenous groups are linking up with more experienced transnational actors

Result: Multiple, small networks, loosely coupled

Independent planning and execution of attacks

Local groups may have LITTLE or NO ELECTRONIC CHATTER as in the Madrid bombing of March 11.

Loosely Coupled, Federated and Fuzzy Networks

Effective terror networks have:

- Good LOCAL KNOWLEDGE to know the potential targets, their weaknesses and difficulties
- TRANSNATIONAL CONTACTS to provide materials and expertise unavailable locally

London, July 10, 2005

- SUFFICIENT TRADECRAFT to maintain cover of not only their activities, but also their TIES to other groups

TIGHT COUPLING, HIERARCHICAL C2 would make these networks easy to take down

The Problem of Terror Networks

- Distributed, flexible, agile command structure
- Cellular structure is “self-healing” after attack
- Small footprint of sub-structures (Sleeper cells, Operational cells, Command Cells) make them difficult to find
- Global-spanning technologies allow networks to be spread sparsely over large territories, provide exceptional cover

Advantages of Network Organization:

The Strength of Weak Ties

Network organization reduced limitations of terrorist organizations and improved their robustness

- Augmentation of manpower
- Pooling of expertise and experience
- Improving access to critical resources
- Shortening critical paths to goals
- Creation of useful redundancies

Result:

Network Organization Becomes a Force Multiplier

Computational Social Science

Computational Social Science is an emerging, hybrid discipline that is focused on rendering social theory into computational constructs for the following purposes:

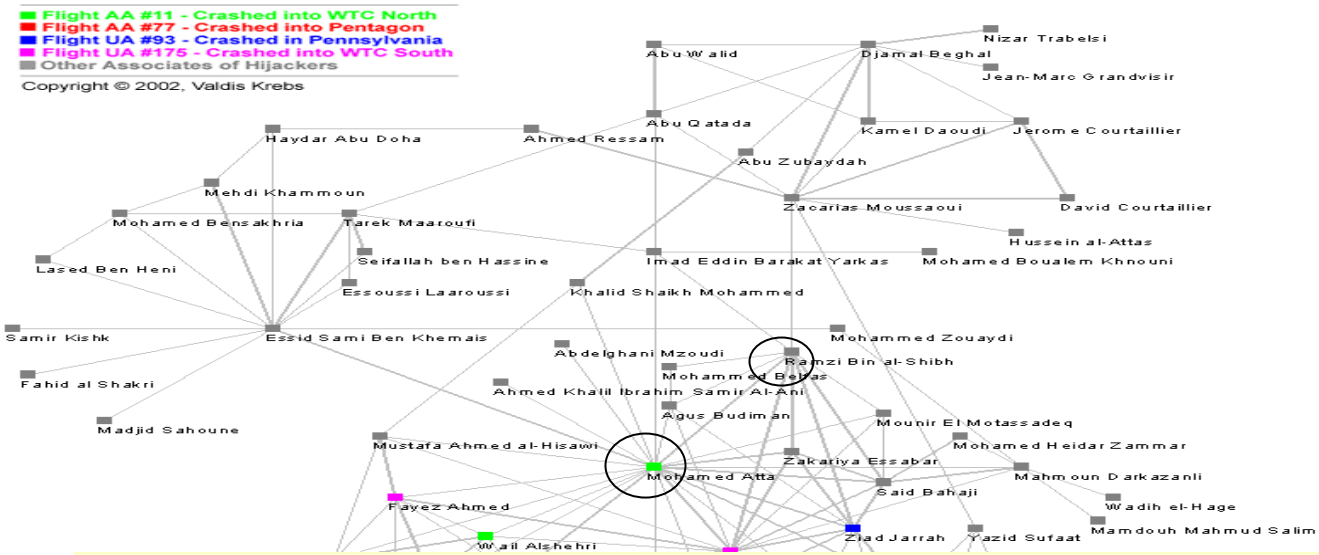
- To **investigate and experiment** in situations where direct observations of human behavior is not possible or not ethical
- To **develop new theory and new insights** that can be applied from the artificial to the natural world

Social Network Analysis

- A **methodology** that is very simple to cast into computational terms
- Deals with connections of **people to people**, **people to resources**, **people to events**, and other connections for the purpose of understanding how humans behave in formal and informal settings
- Strongly mathematical with well validated metrics
- Large body of ethnographic data to support its theory

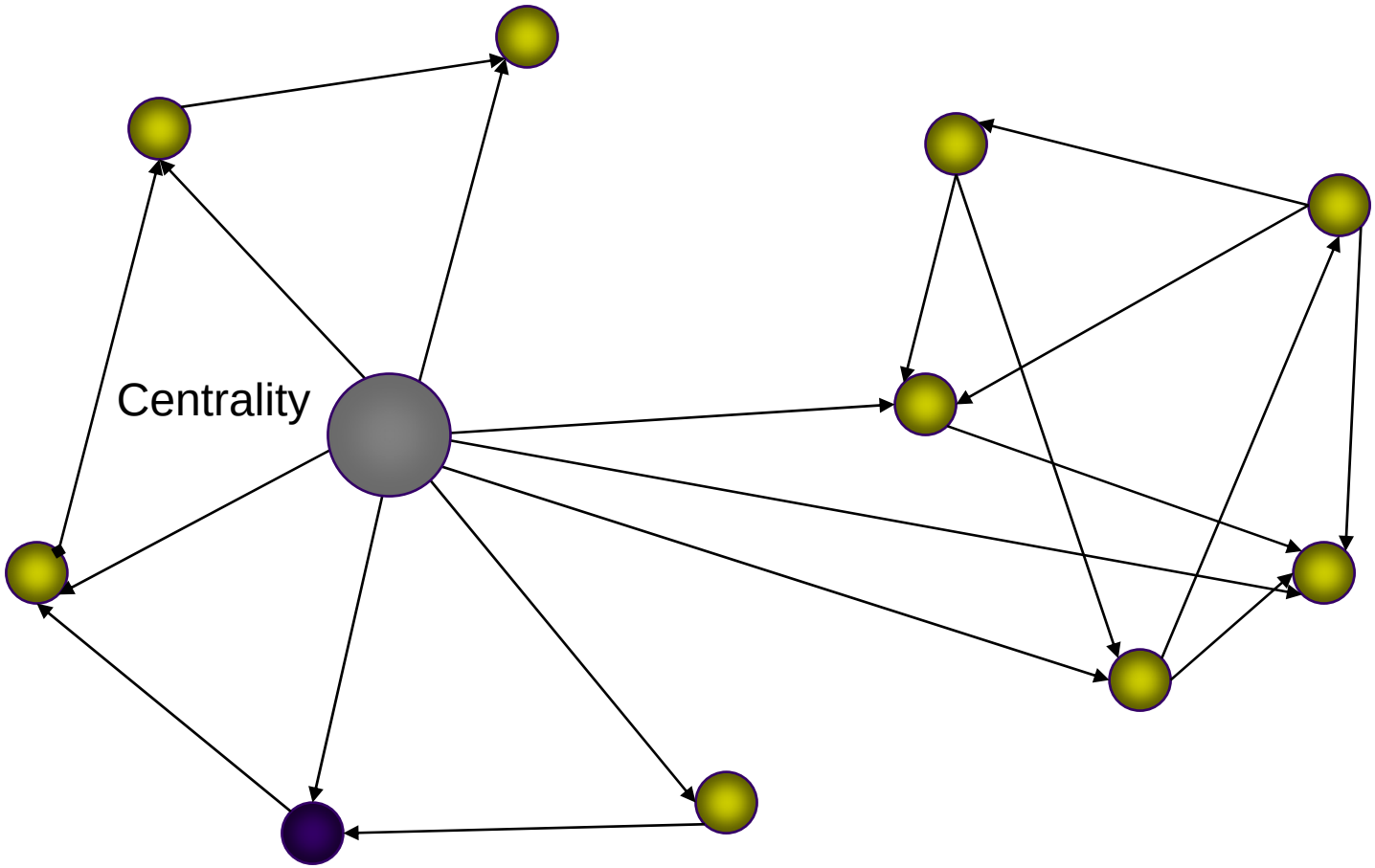
Sparse Networks are Easy to Read and Intuit

September 11, 2001



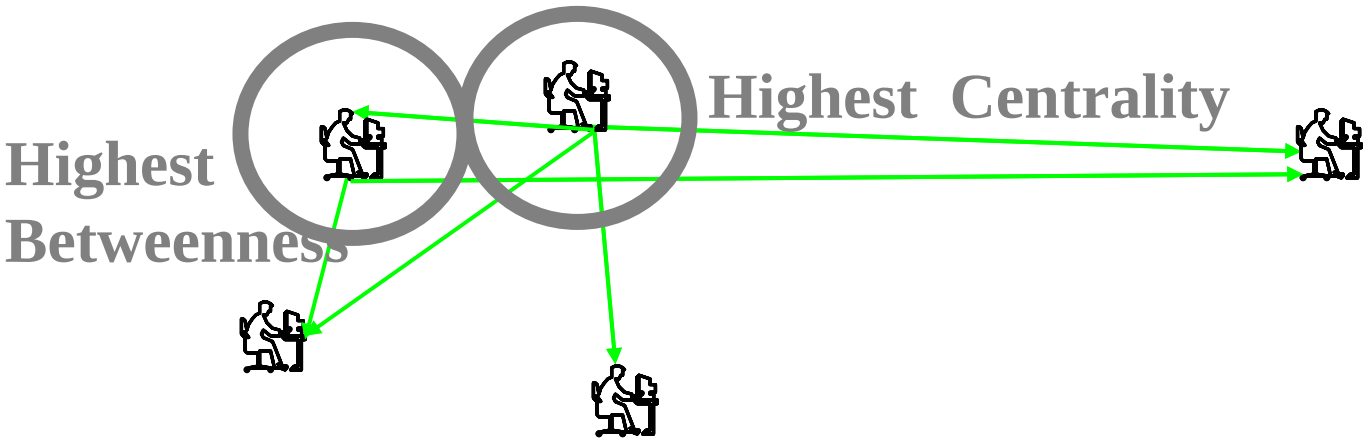
- WHO is important?
- WHY are they important?
- WHAT kinds of vulnerabilities can SNA identify?
- HOW can the military use (often incomplete and faulty) network data to disrupt, destabilize and contain networked opponents?

Who Is “Key” ?

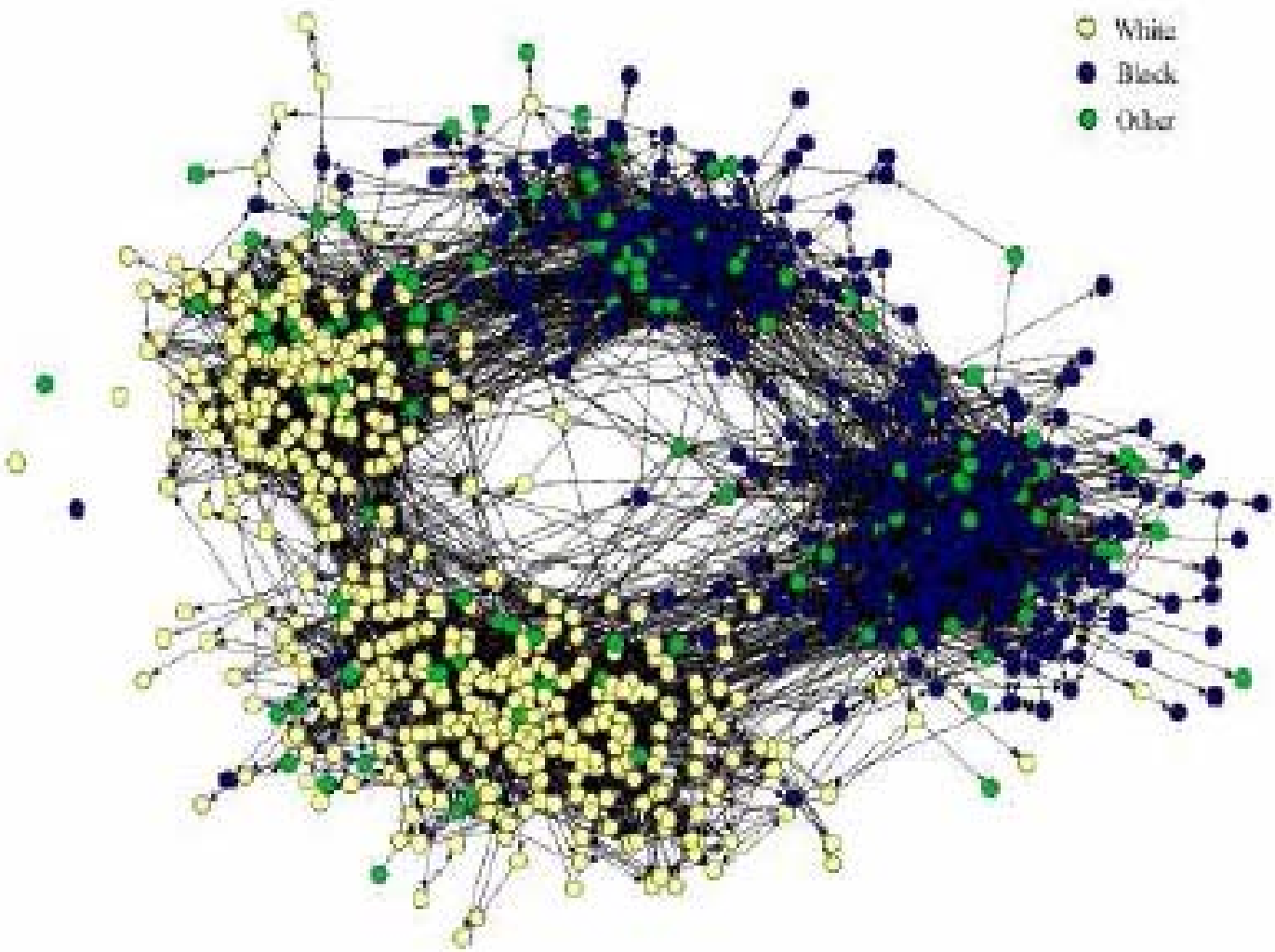


Destabilizing the Network = Removal of Key Actors

Destabilize the Network



Complex, Dense Networks Require Statistical Tools



So – why is this hard?

- The Network
  - Vast quantities of data
  - Multi-mode – people, events, etc.
  - Multi-plex – many connections e.g. financial and authority Aliases (typos, etc.)
- The Information
  - Intentional misinformation
  - Inaccurate information
  - Out-of-date information
  - Incomplete information
- Dynamic
  - Learning, Recruitment, Attrition affect structure

ONR's Support of Seminal Work in Network Destabilization

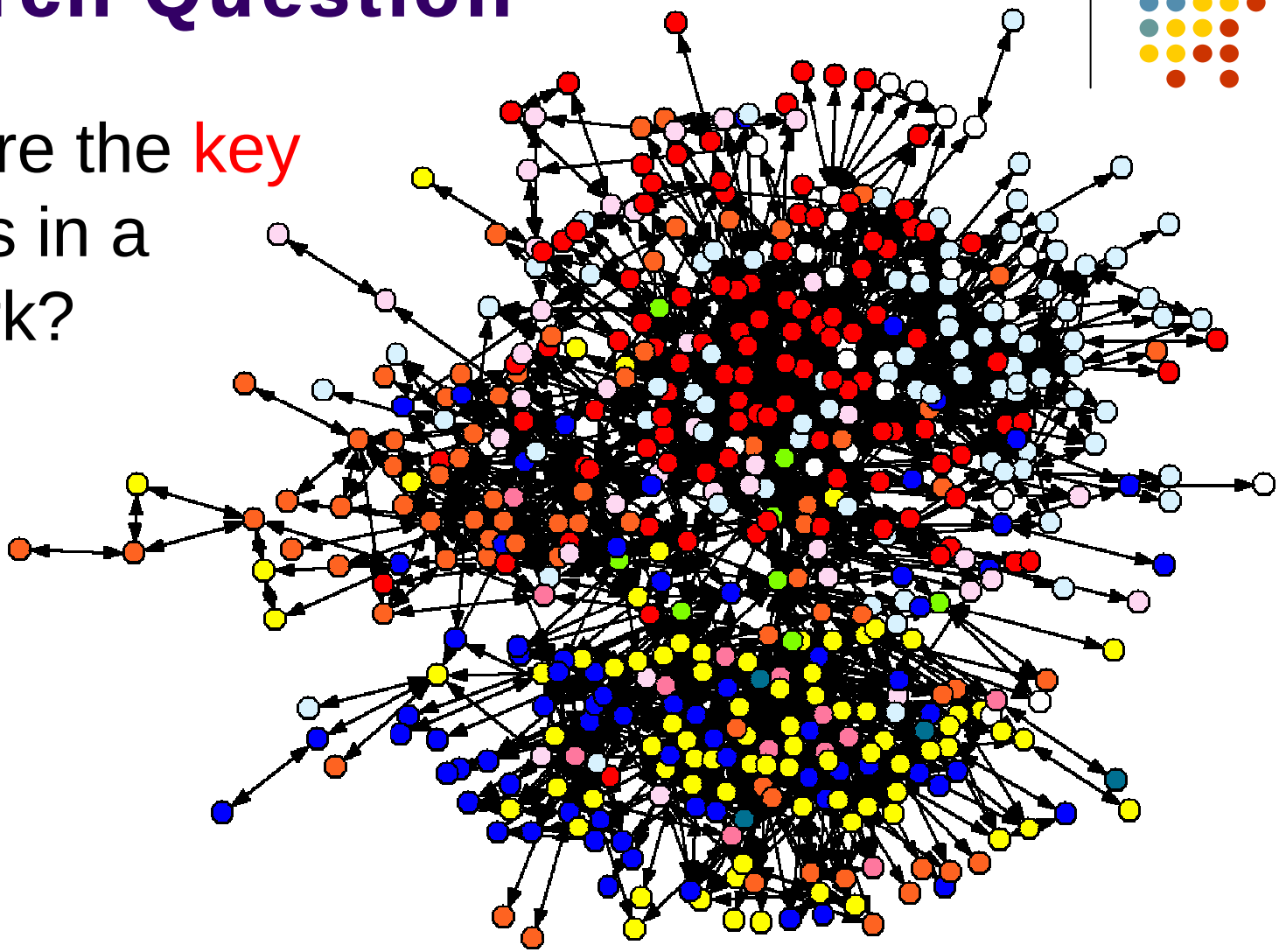
- Removal of top leadership all at once initially caused problems but in network structures, the network was able to recover quickly and become more efficient.
- Removal of central individuals was also surmountable
- Removal of emergent leaders next "best" strategy for making network less efficient
- **BEST STRATEGY was to remove random nodes (individuals) over time**

Ref: Kathleen M. Carley, Ju-Sung Lee and David Krackhardt (2001). "Destabilizing Networks," Connections, 24 (3):31-34.

- IMPACT: <u>Carley's work shows the clear utility of military-relevant SNA models to rapidly and economically depict destabilization strategies against covert networks.</u>

KeyPlayer Research Question

- Who are the key players in a network?



What specific problems do we need to solve?

- Network Disruption problem
  - How to maximally disrupt the functioning of a network by intervening with the key players
    - E.g., removing them
- Network Influence problem
  - How to maximally spread ideas, misinformation, materials, diseases, etc. by seeding key players
- Network Surveillance problem
  - How to efficiently learn what the network knows by surveilling key players.

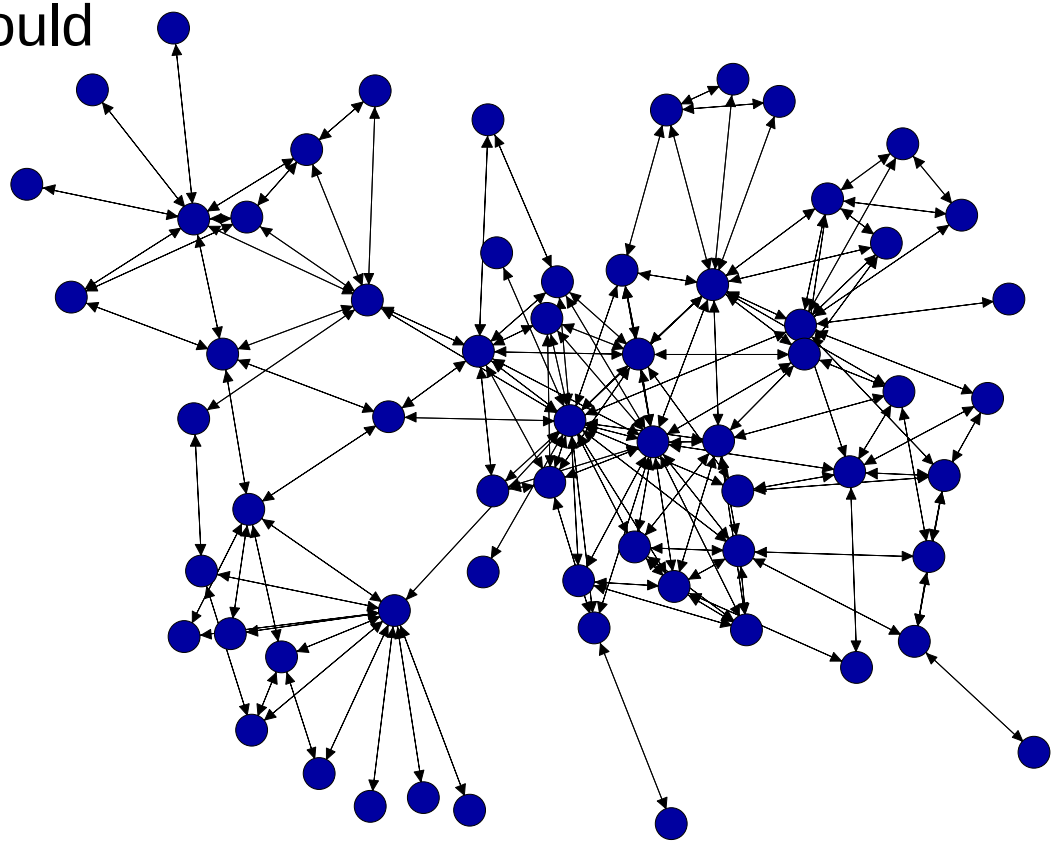
Same under certain conditions

Applications

DISRUPTION		INFLUENCE
Who/how many to **immunize or quarantine** in order to slow spread of infectious disease	Health Care	Selecting peer health advocates for **diffusing** safe practices (e.g. bleaching) and material
Who to **arrest or discredit** to disrupt criminal networks	Criminal Justice	Who to “turn” or feed **false information** to
Where is an organization most vulnerable to **turnover**?	Management	Select subset of employees for **intervention** prior to change initiative

Empirical Example #1
Disrupt Terrorist Network

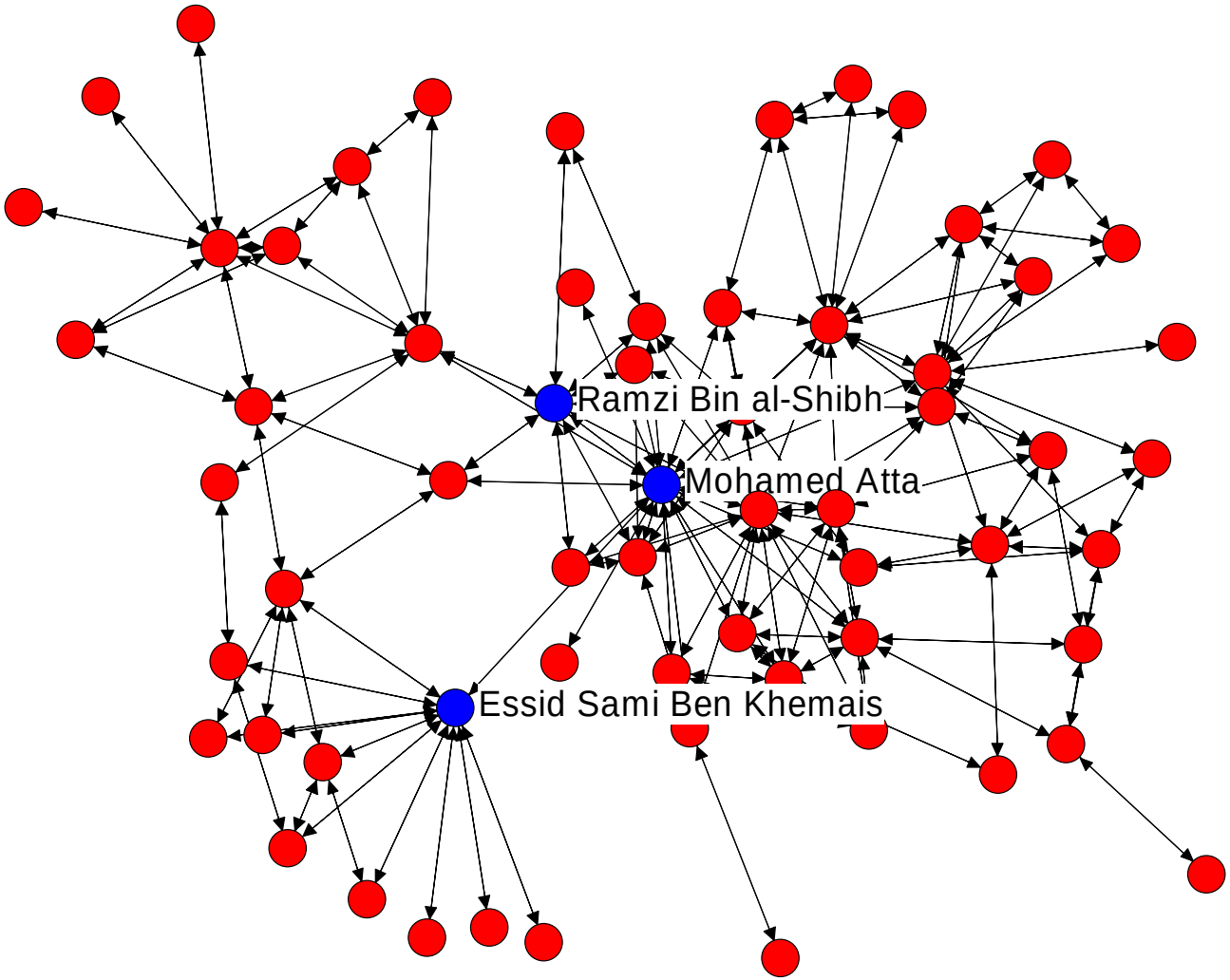
- Which three nodes should be isolated in order to maximally disrupt the network?



Data from: Krebs, V. 2002. Uncloaking terrorist networks. *First Monday* 7(4): April. http://www.firstmonday.dk/issues/issue7_4/krebs/index.html

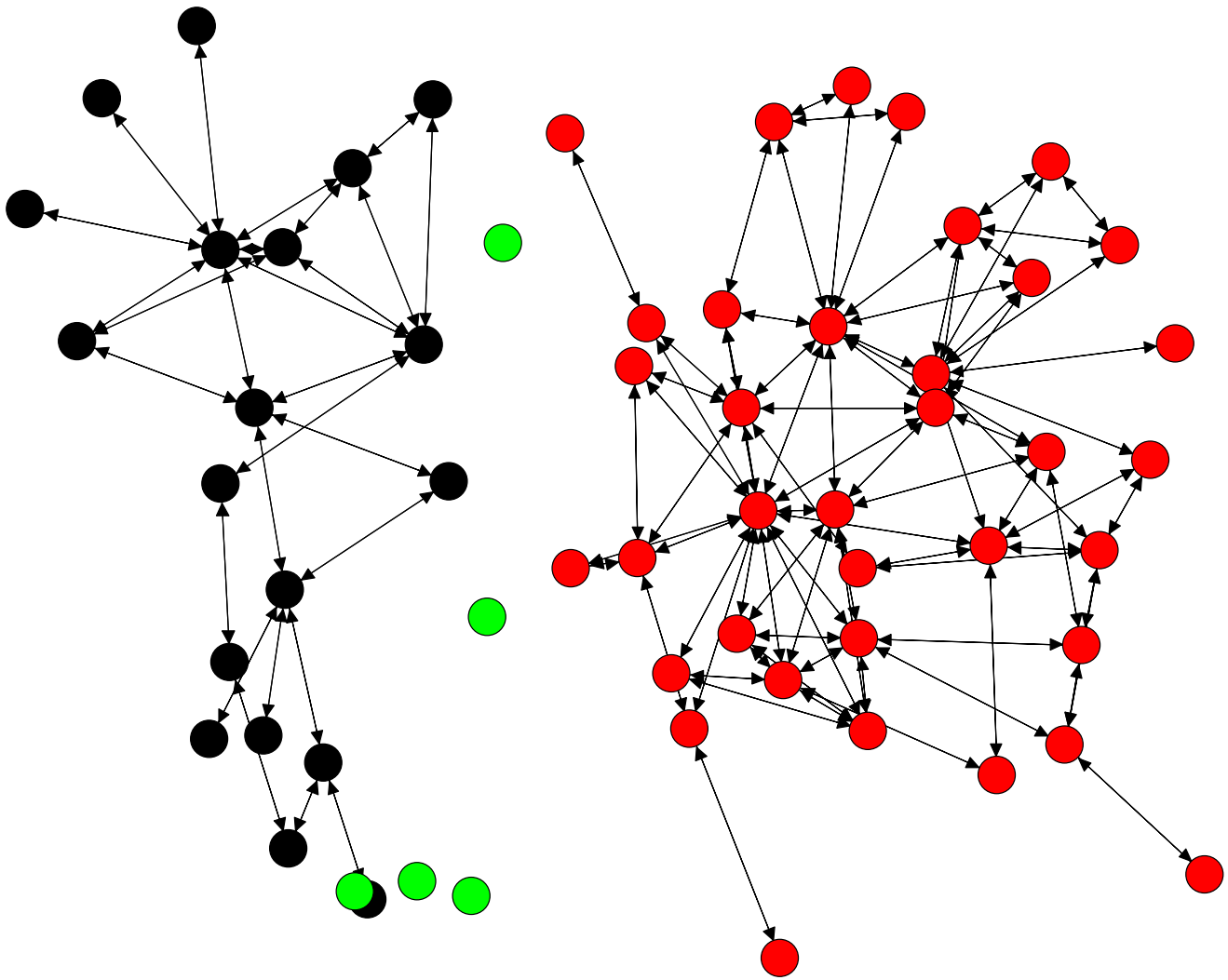
DISRUPTION

KeyPlayer Solution



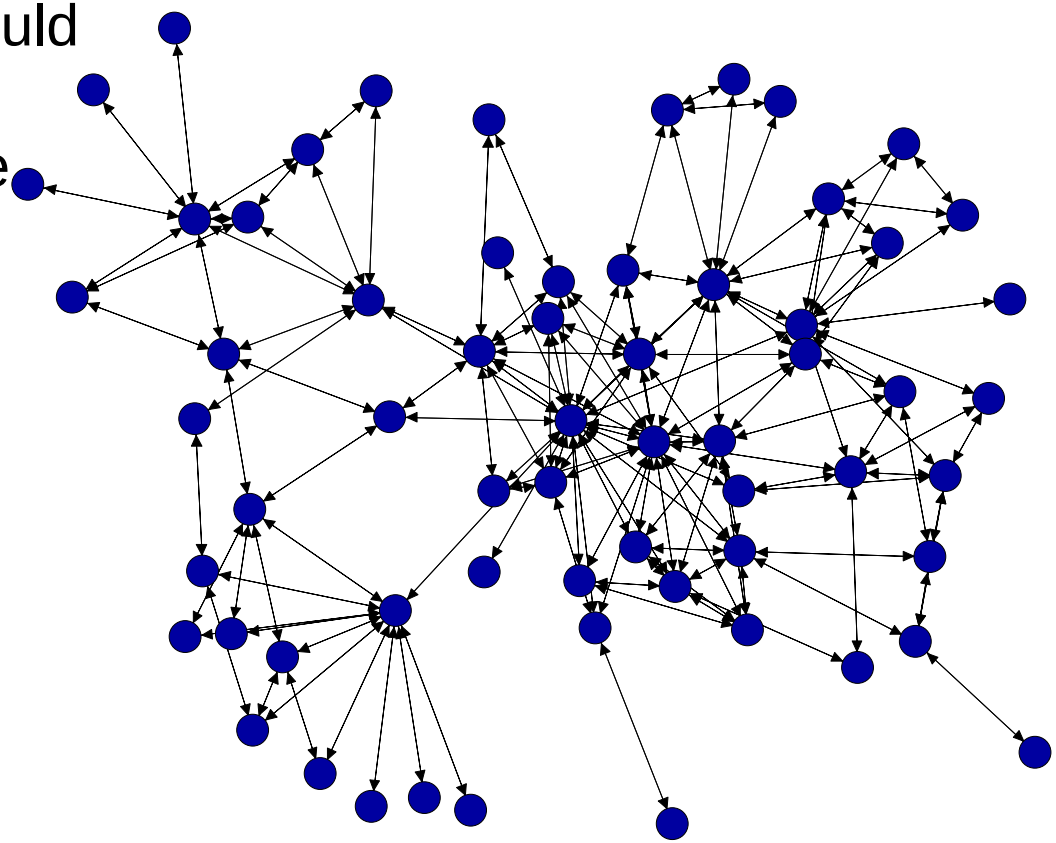
DISRUPTION

KeyPlayer Solution (key players removed)



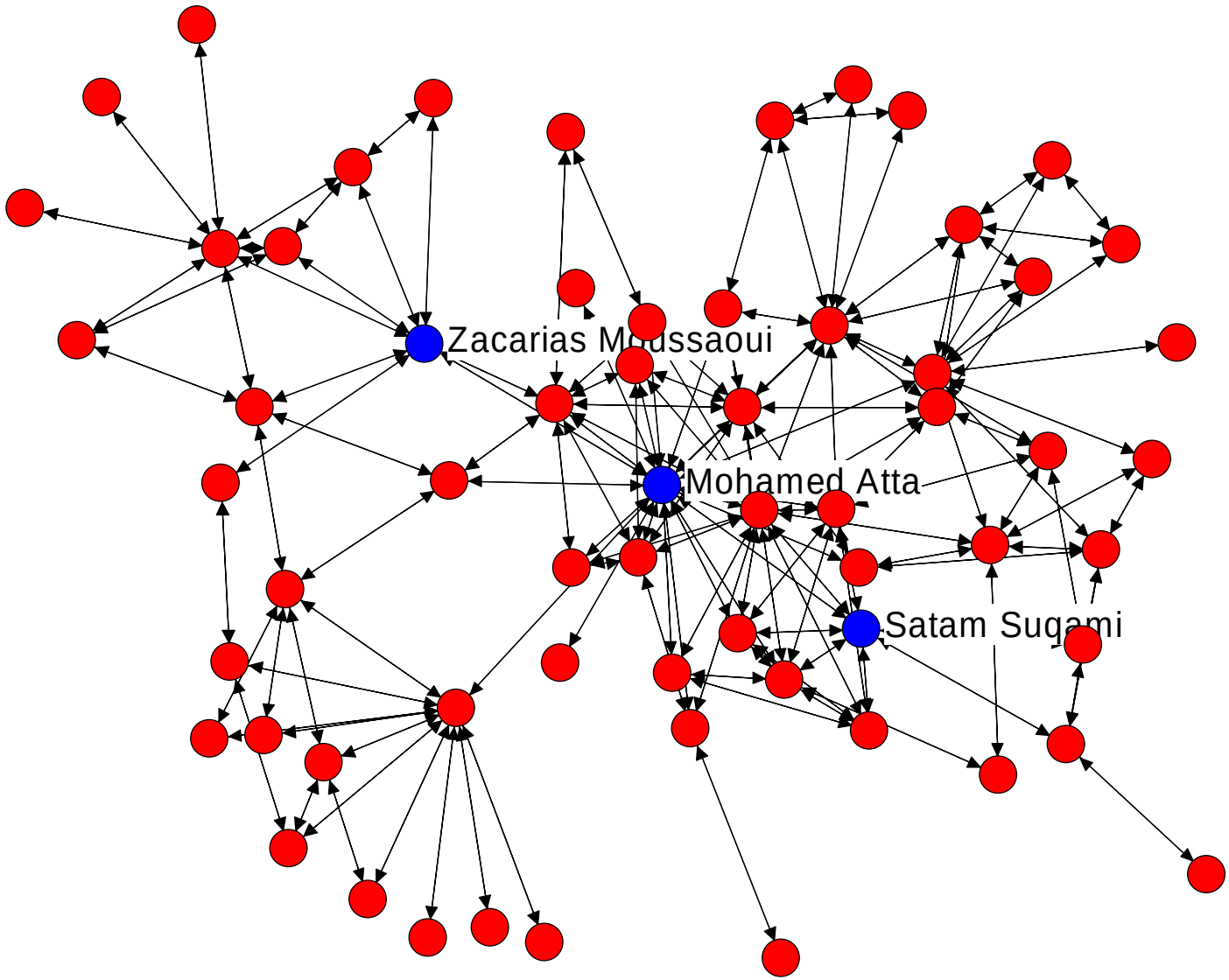
Empirical Example #2
Influence Terrorist Network

- Which three nodes should be selected in order to maximally influence the network by turning / planting information, etc.?



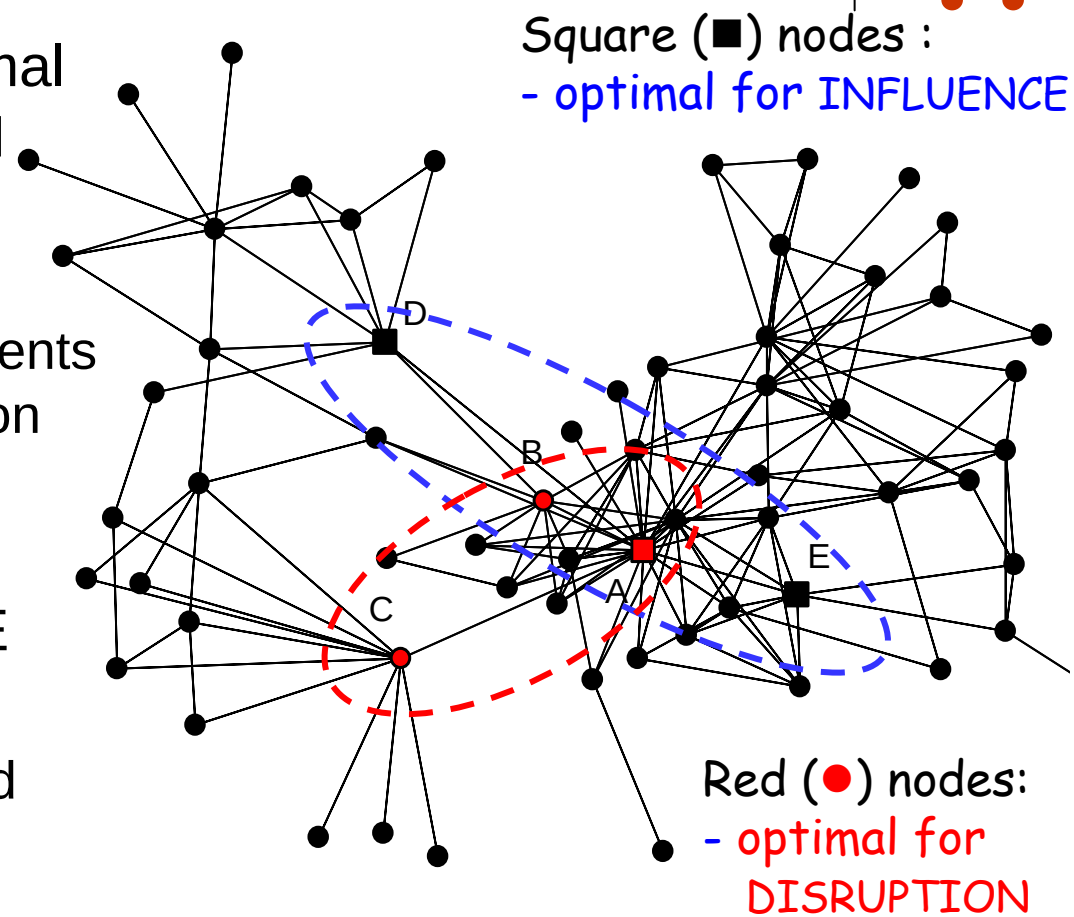
Data from: Krebs, V. 2002. Uncloaking terrorist networks. *First Monday* 7(4): April. http://www.firstmonday.dk/issues/issue7_4/krebs/index.html

KeyPlayer Solution



Terrorist Network Disruption

- Red nodes identify optimal choice for DISRUPTION problem
  - Removing them splits network into 7 components and yields fragmentation metric of 0.59
- Square nodes identify solution for INFLUENCE problem
  - The best nodes to seed with disinformation



Data from: Krebs, V. 2002. Uncloaking terrorist networks. *First Monday* 7(4): April. http://www.firstmonday.dk/issues/issue7_4/krebs/index.html

Main Points

- Computational social science has great things to offer in the analysis of terror networks
- Much of what we want to know about terror networks involves social behavior, rather than culture per se
- Better cultural knowledge will, however, substantively improve computational social science models of terror networks

Incorporating additional information

- Weighting actors
  - By importance, skill, rank etc.
  - By availability, ability to influence, convenience
- Separating nodes with complementary skills
  - E.g., a fragmentation of a network that separates nodes with complementary skills or interdependent roles is better than other fragmentations, all else being equal
- Handling multiple social relations simultaneously
- Ignoring nodes marked as “untouchables”
  - E.g., nodes that we know can’t be reached

LOCAL to GLOBAL variations: Some New Research Questions

- How do local discourses, sensibilities, and issues differ from the discourses and values promoted by transnational sources? (Can those differences be exploited?)
- How is terrorism justified within local contexts?
- What discourages local movements from pursuing violent action? What promotes violent action? What factors vary culturally?
- Are there variations in the way local movements use new media and technology (i.e., webpages, SMS, chatrooms, blogs)? Where is new media important?
- How do terror networks vary from culture to culture, in terms of configuration, command and control, secrecy, and cross-group cooperation?