Knowing the Enemy: A Simulation of Terrorist Organizations and Counter-Terrorism Strategies

Maksim Tsvetovat
Carnegie Mellon University
maksim@cs.cmu.edu

Kathleen Carley
Carnegie Mellon University
kcarley@ece.cmu.edu

Abstract

Given the increasing threat of terrorism and spread of terrorist organizations, it is of vital importance to understand the properties of such organizations and to devise successful strategies for destabilizing them or decreasing their efficiency. However, intelligence information on these organizations is often incomplete, inaccurate or simply not available – thus making a study of terrorist networks more difficult. In this paper, we propose a methodology for realistically simulating terrorist networks for the purpose of developing network metrics specific to the terrorist networks and testing strategies for destabilizing them.

Contact:
Maksim Tsvetovat
Dept. of Social and Decision Sciences
Carnegie Mellon University
Pittsburgh, PA 15213

Tel: 1-412-519-4304
Fax: 1-412-268-6938
Email: maksim@cs.cmu.edu

Key Words: list up to 8

Acknowledgement: if any
Support: This work was supported in part by the National Science Foundation under the IGERT program for training and research in CASOS, and the NSF KDI IIS-9980109. Additional support was provided by CASOS - the center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research, the National Science Foundation, or the U.S. government.

Knowing the Enemy: A Simulation of Terrorist Organizations and Counter-Terrorism Strategies

Maksim Tsvetovat and Kathleen Carley

Given the increasing threat of terrorism and spread of terrorist organizations, it is of vital importance to understand the properties of such organizations and to devise successful strategies for destabilizing them or decreasing their efficiency. It has been widely noted that terrorist organizations (as well as many other secret or illegal organizations) are very rarely built on the same organizational principles as legitimate organizations [Garreau 2001]. While legitimate organizations tend towards building hierarchical structures and chains of command, the illicit organizations must strive to maximize secrecy and security.

The need for security dictates that terrorist organizations must be structured in a way that minimizes damage to the organization from arrest or removal of one or more members [Erickson 1981]. This damage may be direct – making key expertise, knowledge or resources inaccessible for the organization, or indirect – exposing other members of organization during interrogations. Thus, an organizational network emerges that combines massive redundancy with secrecy, separating into densely connected cells that are sparsely interconnected with each other. No clear hierarchy emerges from observation of these networks, other then a definite role of a cell leader, who is often the only contact that the cell has with the outside world.

During investigations, it is often reported that the perpetrators of a crime were loners and made little contact with the outside world, thus minimizing the visibility of the network and the chance of leaked information. Conspirators within illicit organizations rarely form outside social ties and often minimize the activation of existing social ties inside the network. The cells are interconnected via strong ties, such as familial relations or ties formed during training. Yet, unlike normal social networks, these ties remain mostly dormant and therefore difficult to discover. They are only activated when absolutely necessary. Thus, the terrorist networks balance a need for secrecy with the redundancy they need to survive in a hostile environment.

The best profile of structure of terrorist networks, based on publicly available data, is the following [Carley & Lee 2001]:

- The network consists of cells with very low interconnection between cells
- Internally, the cells exhibit high degree of connectedness and all-to-all communication patterns
- There is a very low probability of a tie occurring by chance (0.007)
- The probability of triad closure (link from *x* to *y* being more likely if both *x* and *y* are linked to third party *z*) is 0.181
- Senior members of each of the cells are often also parts of other cells and interact with other senior members on the network.
- Cell leaders are more knowledgeable then other members
- Cell members have distributed knowledge
- Cells use information technologies and electronic communication.

As is the case with many criminal networks, the analysis of terrorist networks can be complicated by a number of factors [Kerbs 2001], including:

- Incompleteness – the missing nodes and links not uncovered during the investigation. Information is particularly incomplete before a terrorist cell goes into action – only very sparse data may be available
- Fuzzy boundaries – the difficulty in deciding which nodes constitute active parts of the network and which constitute noise
- Dynamism – the terrorist networks are always changing due to secrecy requirements. Thus, links may be activated and deactivated too quickly for the investigation to notice.

Given constraints imposed upon investigators of terrorist organizations, we propose that a computer simulation can be built to understand the nature of terrorist organizations and to develop effective strategies for combating them.

Simulation Architecture

To simulate the activity of a terrorist organization as well as investigative work of a police organization, we are using a multi-agent network simulation methodology. The methodology is based on the following assumptions:

- The simulation consists of agents: independent, autonomous entities endowed with some intelligence
- Agents are cognitively limited
- Agents can learn knowledge about the world and referential knowledge about other agents, with a limited learning capacity
- Agents can forget
- Agents communicate asynchronously and deal with asynchronicity (i.e. deadlocks, delays, etc) in an autonomous manner.
- Agents do not have accurate information about the world
- Agents do not have accurate information about other agents
- Instead, agents form beliefs about the world and other agents based on history of interactions (i.e. transactive memory)
- Agents do not use predefined geometrical locations or neighborhoods.
- Agents are located on free-form graphs representing their social network, resulting in a structural realism that is greater then that of grid-based simulations
- Agents can form an arbitrary number of networks, depending on the simulation domain.

Simulation Parameters

While the above assumptions apply to all multi-agent network models, a number of specifications are specific to the domain of simulating terrorist organizations:

- The simulation consists of two teams of agents: the terrorist agents and the police agents.
- The network of the terrorist organization is closely modeled upon existing information about structure of real-world terrorist organizations
- Terrorist agents perform a trinary classification task: identifying objects as friendly, hostile or neutral.
- Agents' performance in this task depends on the knowledge and resources an agent possesses.
- Knowledge can be exchanged within agent's social network neighborhood
- If an agent lacks resources to complete a task, it may delegate it to another agent that may have them
- Efficiency of the organization is measured in terms of number of tasks that have been completed correctly.
- If a link within the terrorist network is disrupted or a node is removed, agents may try to rebuild the network by creating new ties. However, this takes time if the original network was not redundant.
- A number of police agents are dedicated to reducing the performance of the terrorist organization by finding key nodes in the terrorist network and isolating them.
- Terrorist agents' communications can be wiretapped by the police agents. The wiretaps are not perfectly efficient, resulting in the investigators only having access to partial information.

Police agents can isolate or immobilize a terrorist agent and obtain parts of its knowledge about the terrorist network via interrogation. However, isolating a terrorist is an expensive activity (given the political, legal and operational constraints), thus making it desirable to achieve maximum effect on the functioning of the terrorist network while isolating the minimum number of agents.

To identify terrorist agents to be isolated, police agents build a model of the terrorist network using information from wiretapped communication, and use one of a number of strategies to identify important nodes on the terrorist network, including

- Network centrality
- Betweenness
- Amount of unique knowledge an agent possesses

- Cognitive load – a combination of amount of communication an agent handles, number of tasks it completes and amount of knowledge that it has.

The simulation experiments are designed to test the impact of different isolation strategies and wiretap strategies on performance of the terrorist organization. A number of intelligent strategies are compared to a baseline strategy of isolating random agents.

Preliminary Results

In an experiment we have simulated a group of terrorists with the following characteristics:

- The organization consists of 50 agents
- Agents are organized into cells with a mean cell size of 6
- Agents are trying to complete a series of knowledge-intensive classification tasks as described above.

To observe the essential effect of anti-terrorist policy, the police agents are allowed to collect data on a terrorist network for 50 time periods, and then isolate exactly one agent from that organization. In one experiment, the police agents pick a random agent to isolate, and in the next experiment they isolate the agent with highest centrality.

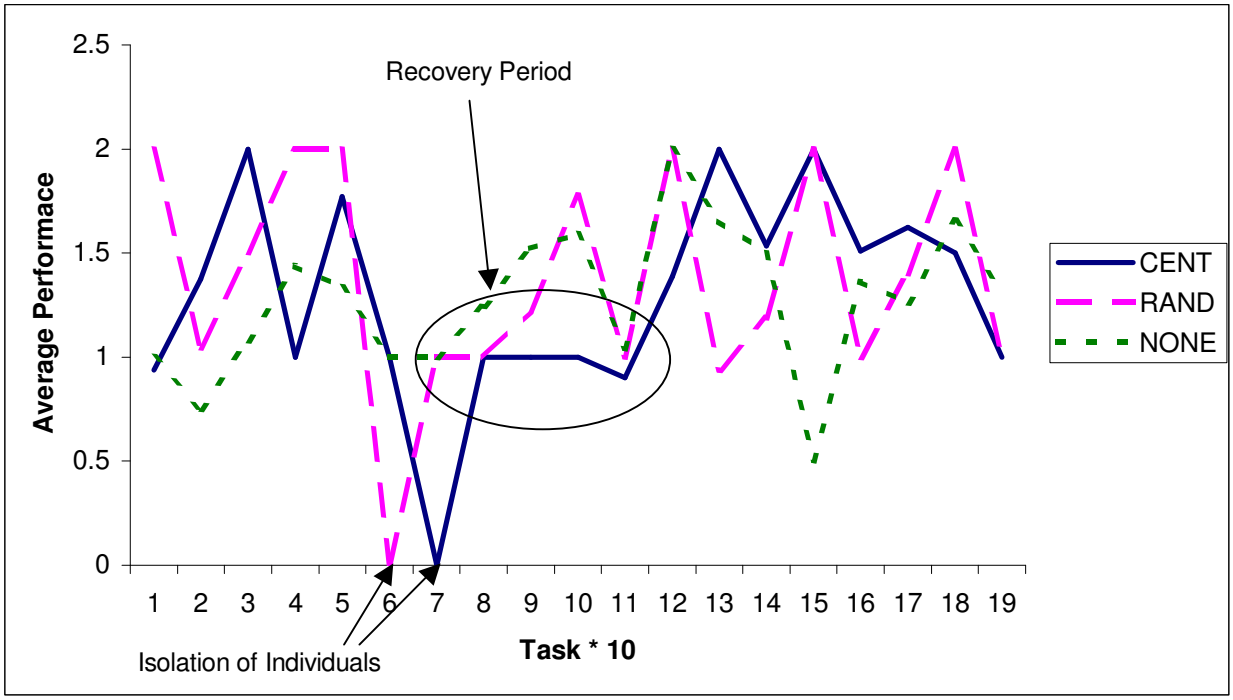

Figure 1: Performance of Tasks by Terrorist Agents in Presence of an Anti-Terrorist Strategy

As Figure 1 shows, isolation of one member of a terrorist network does not have a permanent effect upon the performance of the organization. In time, the organization recovers and restores its normal level of operation. However, when an agent with the highest centrality is isolated, the recovery time is much greater then with isolation of random agents.

In the full paper, we also present the effects of wiretapping strategies and effects of accuracy of estimation of the structure of the terrorist network upon the performance of the police agents (measured by degradation of performance of the terrorist organization).

References

[Kerbs 2001] Valdis E. Kerbs, 2001, "Mapping Networks of Terrorist Cells", *Connections*, 24(3): 43-52

[DIA 2000] Defense Intelligence Agency, 2000, "Criminal Network Analysis Training Course", http://www.oss.net

[Carley & Lee 2001] Kathleen Carley & Ju Sung Lee, 2001, "Destabilizing Terrorist Networks", (reference?)

[Erickson 1981] Bonnie H. Erickson, 1981, "Secret societies and social structure", *Social Forces* 60(1): 188-210

[Garreau 2001] Joel Garreau, 2001, "Disconnect the Dots", *Washington Post*, September 14, 2001, Page C01