A Graduate Student Project:

Predicting Political Party Propensity for Violence using Game theory and Attack Graphs

Henry Hexmoor, SIUC

July 2010

Human social networks might turn to violence as an aberrant response to state actions taken to control them. We model this as a two player non-cooperative game. One player is the authorities dubbed as *the state*. The other player is the collective mind of the network, dubbed as *the gang*. At times, the gang will be inclined to use violence as a signal for its displeasure with state control. The state chooses one target from a set of possible targets and attempts to reach it, whereas the gang must determine which target has been chosen and defend it. We assume that the target is known only to the state. The gang knows the set of possible targets without being certain which target has been chosen by the state. In addition, the gang is limited to execute only preemptive actions, i.e., violent actions that can prevent attacks only when executed in advance. The notion of *attack graph* captures the intuition about possible attacks that can be launched against a set of targets.

Given a set of agents, size *n*, each pair of agents is initially connected guided by a parametric, stochastic value. Links will be bidirectional but lack reflexivity. Links are used as the only means of information exchange. A message is transmitted through a link between nodes A and B only once. Although a link lacks direction, in a given time unit a message is sent once from a sender to a receiver without concern for acknowledgement. For simplicity, we do not consider transmission failures. Transitivity property is a node property that can be set to on or off. With on, an exchange hops one unit on its own. With off, information exchange is dyadic. Information received stops going forward. Transitivity is a global property that can be set for every node as a toggle switch value; i.e., all nodes on or all nodes off. Transitive information exchange is hyperdyadic, i.e., going beyond a pair of communicating nodes.

Network architecture, i.e., topology or structure is the shape of the network. It is user determined. Initial two topologies are either random and scale free networks (Newman, et. al., 2006). Scale free networks were first proposed by Albert Barabasi to reflect the power law distribution of connections (Barabasi, et. al., 1999).

To study the evolution of the network from this initial state, each agent will be randomly assigned *k* unary attributes (e.g., these could be seen as actor ideology or type) that will affect their affinity to each other.

Homophily will be used to bind nodes. Pairs of connected agents who share multiple attributes will consummate their link by force of homophily, while other links will be dissolved due to lack of adequate homophily, thus allowing us to study network evolution.

We will model the impact of the network on tactical action by initially randomly assigning each actor to one of two political stances (i.e., opinion) -- violence or concession. We will then model changes to these individual states as a function of network interactions that are modeled in terms of simulated, exchanges of political stance among linked pairs. This will be studied using a period of parametric time period, *T*, that will be used to simulate T distinct exchanges. It is commonly known that influence among individuals dissipates after three degrees of separation (Christakis and Fowler, 2009). Therefore, T will be assigned a number > 3. Within (n-1)*T time units, information will reach the periphery of the network. With a hypothetical X nodes (X < n) leading original opinions, we will need X* (n-1) * T time units to inform all nodes. If X = n, initial time spread phase will be n* (n-1) * T. Transivity will speed the spread.

In dyadic communication, Contagion will be limited to neighbors (i.e., one degree of separation), thus ensuring that the network is part of the evolution. Individuals will increment opinions they receive from their neighbors. If the opinions are the same as their own, they strengthen their original stance. Otherwise, if the balance of opinions overwhelmingly differs from their own, they will change. A global, default parameter will be used to determine the threshold of opinion stubbornness in the population.

We will run our simulation by adjusting parametric values and examine the effects of network structures. Keeping all else equal, we hypothesize that scale free networks will spread opinions faster than random networks. Beyond this initial experiment, we will vary other parameters such as the level of centralization in the original social network, levels of initial ideological conditions, stability of the terror network that evolves (especially to random perturbations and interventions aimed at different elements of the network), and the density in initial networks.

References

A.L. Barabasi, Albert, Jeong, 1999. Mean-field theory for scale-free random networks Physica A 272 (1999) pp. 173-187, Elsevier.

D. Berger, 2005. Outlaws of America: The Weather Underground and the Politics of Solidarity, AK Press. C. Davenport, 2007. State Repression and the Domestic Democratic Peace, Cambridge University Press

N. Christakis, and J. Foler, 2009. Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives, Little, Brown and Company.

S. Jha, O. Sheyner, and J.Wing, "Two formal analyses of attack graphs," in *Computer Security Foundations Workshop (CSFW)*, Nova Scotia, Canada, 2002, pp. 49–63.

J. Nash, "Equilibrium points in n-person games," vol. 36. Proceedings of the National Academy of the USA, 1950, pp. 48–49.

M. Klein, 1995. The American Street Gang: Its nature, Prevalence, and Control. Oxford University Press.

J. Nash. 1950. Equilibrium Points in n-Person Games, In *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 36, No. 1. pp. 48-49.
M. Newman, A.L. Barabasi, and D. Watts, 2006. The Structure and Dynamics of Networks, Princeton University Press.
M. Osborne, 1994. An Introduction to Game Theory, MIT Press
L. Swiler, C. Phillips, D. Ellis, and S. Chakerian, Computer-attack graph generation tool, in *DARPA Information Survivability Conference and Exposition*, Anaheim, California, 2001, pp. 146–161.

Background: Attack Graphs and GT (Braynov, 2006)
Approach:
1. Use GT to formulate the problem.
2. Use MAS testbeds like netlogo to simulate a prototype.