Paper Title: Modeling the Characteristics of Radical Ideological Growth using an Agent based Model Methodology

Paul Cummings
Krasnow Institute, GMU Computational Social
Fairfax, VA
Pcummin2@gmu.edu

Chalinda Weerasinghe
ICF
Fairfax, VA
Chalinda.Weerasinghe@icf.com

ABSTRACT

Warfare is no longer primarily a function of capital, labor and technology superiority on the battlefield. Rather, warfare has expanded to complex interconnected networks of information that can shape the outcome of conflict, on and off the battlefield. In the case of "hearts and minds" warfare, the Internet and social media has been used to share and often spread information in order to produce negative propaganda towards the conflicting parties. (Berman, Shapiro and Felter (2011) Using modern and highly prevalent methods of interaction, terrorist organizations continuously expand their networks through real-time information exchange, enabling operatives to organize, spread information (and misinformation), and recruit new members into their terrorist organizations. As Taspinar (2009) states within his policy publication *Fighting Radicalism*, there are no terrorist societies only conditions for the emergence of terrorist activities. The relative popularity of certain terrorist networks can only be explained within the framework of such radicalized societies where extremist violence finds a climate of legitimacy and implicit support. Such radicalized societies are permeated by a deep sense of collective frustration, humiliation, and deprivation relative to expectations. Terrorists easily exploit this radicalized social habitat. (Ibid)

ABOUT THE AUTHORS

Paul Cummings is Senior Fellow in the Center for Advanced Learning Systems at ICF International. He has over 18 years of technical and management leadership experience in the education, simulation, and training community. Mr. Cummings has been a major contributor to several large research programs where he researched the effectiveness of live, virtual, and constructive training systems. Mr. Cummings currently develops immersive technology systems with an emphasis on behavioral health, social complexity, leadership decision-making, negotiation, and blended learning and assessment strategies. He is also a graduate of the Krasnow Institute Computational Social Science program.

Chalinda Weerasinghe is a research consultant for ICF who specializes in International Relations, Econometrics, Political Economy, and Development Economics. He undertook doctoral studies in Economics and Government and Politics at the University of Maryland, College Park with specializations in econometrics, international relations and development economics. He has an MS in Economics and an MS in International Relations from the Georgia Institute of Technology and a B.S. in Mathematics, Economics and History and Political Science (triple major) from Shorter University. His interests are varied and include topics in pure and applied mathematics, operations research, statistics, and political economy.

Paper Title: Modeling the Characteristics of Radical Ideological Growth using an Agent based Model Methodology

Paul Cummings
Krasnow Institute, GMU Computational Social
Fairfax, VA
Pcummin2@gmu.edu

Chalinda Weerasinghe
ICF
Fairfax, VA
Chalinda.Weerasinghe@icf.com

INTRODUCTION

Generally speaking, definitions of terrorism are composed of similar concepts including violence, fear, and motivation toward change. In its most general form, terrorism can be defined as "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change" (Hoffman 2006a, p. 40). Terrorist organizations can be modeled as social networks where vertices represent members of the organization and edges represent direct communication between members. Terrorist leaders may choose to avoid being involved in direct communication to evade detection. Martonosi et al. (2011) argue that increasing the amount of communication through a key vertex increases that member's visibility to intelligence agencies. Martonosi notes problems arise when disrupting terrorist networks; namely, in the disruption process, we may not have the resources necessary to disconnect the network. Instead, targeting a leader in the terrorist organization could have an equally disruptive effect for lower cost and chance of detection (Martonosi et al. (2011). Therefore, a portion of the research is to uncover how terrorist disruption differs between disconnection and containment. Carley et al (2001,2002b, 2003, 2004) also noted that formal models of network analysis can also suggest where removal of key nodes or vertices can disrupt the organization's ability to transmit commands across hierarchical levels of the organization, thus leading to command degeneration (Butts, 2003a; Carley et al, 2004). The difficulty with this approach is that an important aspect of the dynamics of terrorist networks is that they are learning organizations. In other words, simply removing network information will not guarantee the structure will disintegrate (Hoffman, 1997; Tsvetovat and Carley, 2003). In fact, one of the most insightful inferences of Carley's Dynet model is that rather than concentrating on removing terrorist leaders, a policy of information isolation may better serve to significantly degrade the functioning of terrorist organizations. With this in mind, I propose a model that validates this general premise, but also evaluates additional characteristics such as viewing the network space as a fitness landscape where infiltrators must find optimal locations to thwart the spread of information.

Use of Social Network Analysis to Model Networks

Social network analysis (SNA) provides a visualization of individuals (nodes) and their relationships between one another (links) to form a network structure. In addition to providing visualizations that can uncover hidden relationships or patterns and potentially motivations of behavior, SNA generates metrics that identify the importance or influence of individuals, the strength of ties, and the density and distance of the network. These metrics are useful to understanding influential people in the network and how information flows through a network. For example, shorter path lengths and distance found in more centralized networks can facilitate resources and information much easier, but less centralized networks allow for more adaptability from any kinds of shocks to the network, such as the removal of the leader, and this makes it more resilient. Perliger (2014, p. 49) explains, "successful networks obtain enough hierarchy (level of centrality) to ensure effective coordination and cohesive operational vision, and on the other hand, provide enough freedom and flexibility to its members and subgroups - a practice which ensures survival when some parts of the network become dysfunctional." Terrorist networks must balance that need for effective communication and coordination with information flowing through the network with the need for security and adaptability. In addition to keeping the network secure and efficient, network members must also worry about defection. Dense networks provide an additional benefit of being able to better minimize defection as numerous links can provide a greater sense of belonging, but also a monitoring mechanism. Everton and Cunningham (2015) explain that network density is a result of terrorists recruiting through strong social ties as this provides a security benefit, but requiring too much security can isolate a network to the point of collapse, as they do not have access to necessary information and resources. SNA metrics provide a method to understand the goals of a network and structurally where weaknesses exist. Whether a network is more focused on security or efficiency will determine how adaptable a network is and what kind of disruption strategies will work against it.

The value of social network theory versus other political science and sociological approaches is its focus on the value of the network structure rather than the characteristics of the individual. While social network analysis leaves room for individuals to affect their fate, it argues that the structure of the network and relationships and ties with others in the network are more important. The network structure of an organization (in this case a terrorist organization) will affect its ability to access new ideas, recruit new individuals, and achieve sustainability. Network analysis seems to work because it provides a structural analysis while still leaving room for individual effort. In a sense, network analysis builds upon many organizational theories, since networks are just another organizational structure. As Charles Perrow discusses in his work Complex Organizations, many organizational theories have evolved over time in an attempt to explain the organization structures of the related era.

Evaluating Terror Networks with Social Network Analysis

Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their intelligence data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling. Valdis Krebs was one of the first to collect data using public sources with his 2001 article in Connections. In this work, Krebs creates a pictorial representation of the al Qaeda network responsible for 9/11 that shows the many ties between the hijackers of the four airplanes. After the Madrid bombing in 2004, Spanish sociologist Jose A. Rodriguez completed an analysis similar to Krebs' by using public sources to map the March 11th terrorist network. In his research, he found diffuse networks based on weak ties amongst the terrorists. (Rodriquez, 2011)

DNA and Agent-based Modeling to Understand Terrorist Activities

Some complex systems have the ability to self-organize (Bak, 1996) particularly when the agents involved have the ability to engage in reflection, as do humans. MAS techniques are powerful for thinking through the complexities of these systems. However, the vast majority of MAS systems have dealt with unrealistic or toy problems, have moved agents about on grids, and have ignored the constraints and enablers on human behavior afforded by being embedded in social networks. The past five years have seen the birth of a new field of science – dynamic network analysis (DNA). The science of DNA entails the theory and design of dynamic networks among diverse entities and the study of all phenomena emerging from, enabled by, or constrained by such networks. Entities include both intelligent agents such as humans or robots and artifacts such as events or resources. DNA makes possible the simultaneous evaluation of multiple networks linking diverse entities leading to an analysis of multi-color, multi-link, dynamic graphs. An example is the simultaneous analysis of the social network and the knowledge network for purposes of improved organizational learning (Carley and Hill, 2001).

Evaluation radicalism and terrorism through GIS

Terrorists often seek access to safe havens, whether in neighboring countries or hidden in areas with harsh terrain (such as mountainous or forest- covered regions), at which to prepare and plot attacks (Korteweg 2008, Kittner 2007). Often very little effort is put into studying the geographical nature of the rise of radicalism. Findley notes that evaluating data at the country or region-level omits much of the key geospatial and temporal variation in terrorist attacks (Findley, 2015). In response, our study is motivated by an expectation that GIS characteristics as well as social network and historical cognitive attributes are all key aspects to understanding the rise and spread of radicalism. The physical space aims to produce more insightful results when considering the spread of terrorism in the following ways. Can a model be developed that replicates the conditions for the emergence of radicalized terrorist networks, and what are the methods to compromise or stop spread of the terrorist network? Additionally what are the spatial, temporal, and virtual characteristics that must be modeled to represent this effect and can this be validated with data from radicalized terrorism during the Iraq War?

METHODS

Given human interactions occur geographically and socially, I posit that to properly research a model that can destabilize terrorists' networks, it is first necessary to develop an accurate geographic and virtual space representation, i.e. a Hybrid Space. A Hybrid Space is the conceptual domain where organizations and individuals operate at the intersection of geographic virtual activity spaces. Within this context, the spaces and places are social constructs, in which people exist and interact. In this domain, cyber-terror evolves as a new reality. Information age terrorism now means that spaces of terrorism now become geographic, social, virtual, and perceptual.

I begin with the premise that radicalism begins within a confined area by a small group of radicals, i.e. a "lone wolf". The Lone Wolfs scenario is populated by radical individuals organized into small cells that are highly isolated from the rest of society. They are not embedded in groups of like-minded individuals, and have very few associates of any kind. Operationally a world of such individuals, in terms of our metrics is characterized by high isolation, low clustering, and a low cell size. In this scenario, the bulk of the terrorism risk comes from Lone Wolfs rather than larger formations, even if many or most of the radicals would never ―bite‖, i.e. pick up arms and commit violence. (Genkin, Gutfraind, 2011). Notably, recruiting new radicals is not performed with equal enthusiasm by all radicals; in fact, it is more often the case that some members are more entrepreneurial than others and play a recruiter function, as was the case with Mohammad Sidique Khan and the 7/7 bombers (House of Commons 2006). Additionally not all individuals will have the same level of influence. I therefore model the concept of both influence and vulnerability when considering the design of the model. Therefore the research will focus on a few key and critical elements; the concept of minimal network ties at close proximity, and level of influence of members.

Agents: I represent a community of N individuals each possessing a set of attributes, methods of interaction, geospatial location, and ties to other individuals in the community. All agents are assumed to have similar parameters but are heterogeneous in their representation. For parsimony's sake, agents have values that are often normalized between 0 and 1. Also, each individual has a stance on radicalism and the issue of terrorism; either strongly strongly opposing (pacifist) a centrist position (moderate), or supportive (radical). These states are represented as 0, .5, and 1.0 respectively. Agents themselves have minimal cognitive attributes and rely on simple communication of information with those other agents within their connected network. Each node holds a belief Bn about whether the information being shared by other agents is valid by calculating mean belief Bi from its neighbors, and combining that with its initial belief Bi.

$$Bi = \frac{1}{\mathrm{n}} \sum_{\mathrm{i}=0}^{\mathrm{n}} a_{\mathrm{i}} = 1/n(a_1 + a_2 + . . + a_{\mathrm{n}})$$

$$Bn = Bi * \mathrm{Ni} + B0 * (1 - \mathrm{Ni})$$

A global *node-influence* Ni parameter is included in the equation to calculate the strength of influence of the connected nodes. In other words, if Ni = 1, the node would be fully influenced by its connected nodes, where a value of Ni = 0 would mean it would not be influenced by connected nodes. So we would expect no change in the network when the global parameter Nv is set to 0. Where commonly models use a process of homophily to illustrate that common attributes are more likely to form ties, this model does not assume anything other than sharing information and the importance of shared influence. Radicalism tends to grow and dissolve based on social ties and not on commonality of attributes. It is therefore assumed in the model that a constant spread of ideas can grow more prevalent with agreement amongst agent social ties.

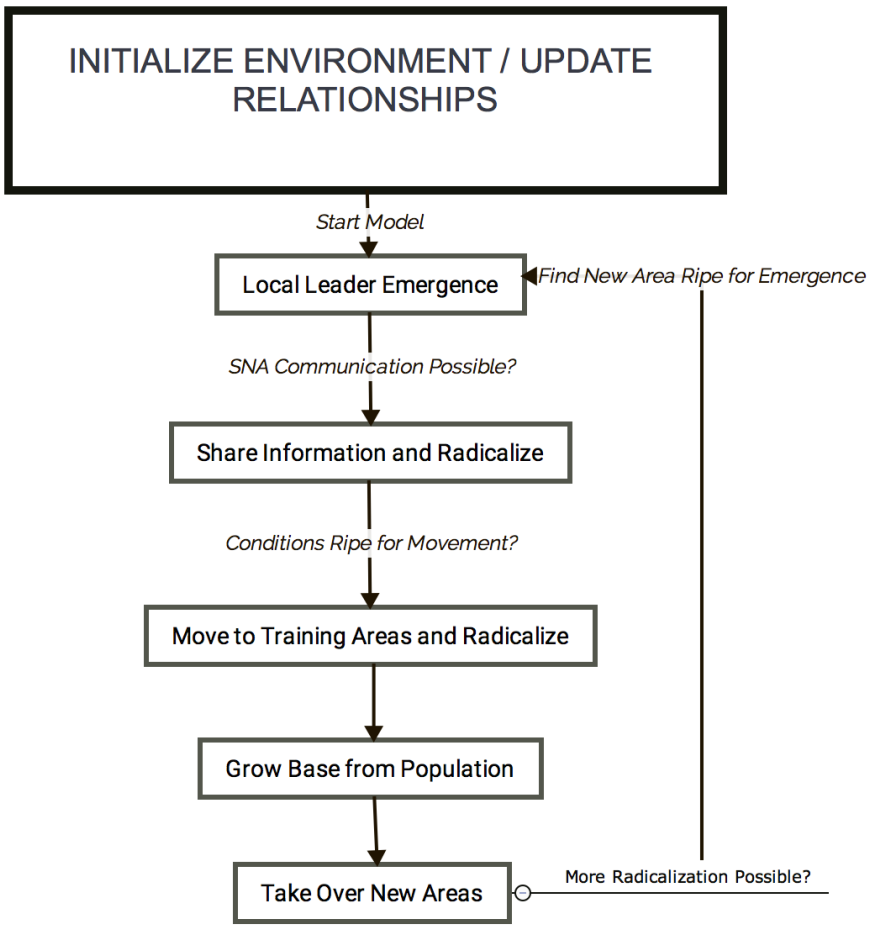


Figure 1: Process Flow Diagram

Simulation Process

The model begins by setting initial conditions as described in Table 1, and each parameter is evaluated through verification procedures towards what I would describe as meaningful although not exhaustive output. At the onset n number of neutral parties exist in the environment with havens and training locations. Havens and training locations are virtual and physical spaces that bolster belief about radicalism by providing additional influence to the agents that are directly connected to them. Through Poisson distribution, random leaders of varying levels of radicalism and influence are activated at time $t < random$ ($leader\_emergence\_parameter$). If a triad or more of agents connected within a cluster reach a specified threshold, growth of radicalism begins to spread within their sphere of influence. The model at an equivalent time period t then finds a new location where a radical leader of with influence can be added to the geographic location. Agents continue to share information, draw consensus on levels of radicalization through agreement, and if appropriate will continue to spread. As agents move to safe havens, the havens and surrounding agents will influence levels of radicals in that region. Additionally if a training area is reached, agents will be further influences (and radicalized) by those within the training area. The training environments (and havens) provide enhanced values for radicalization attendees.

Methods of Verification and Validation

Within the model several parameters and ranges are discussed within Table 1. A sensitivity analysis was executed designed to evaluate the robustness of the results of the model in the presence of uncertainty. This verification process helped to increase understanding of the relationships between input and output variables in a system or model. In order to minimize complexity, model parameters were either normalized between $n = \{0 - 1.0\}$. Verification will also take place looking for syntax, semantic, and run-time errors. In future models, scaffolding assertions that can be helpful in observing outlier values that should simply not occur. Given the abstract nature of the model, verification was limited to perceptive results based on the literature.

Table 1: Simulation Parameters

Description	Value	Verification Method	Results	Discussion
Number of agent types	0-N Each has leadership value (0-1) and vulnerability (0-1)	Examined against literature (Epstein, Genkin)	Verified	3 agent types: Initial Radicals Neutrals Anti-radical movement
Leader emergence	0-number of total terrorists in network	Increase in value increases "total radicalism" within model	Verified linear growth of radicalism with increased leaders	Uses degree measures (SNA) to connect agents. 100% connected to all agents
Terrorist Network Type, Network Topology	Heterarchical (clustered) Hub/Spoke (scale free)	Model will illustrate visual examples of clustered and scale-free networks. Based on existing code model within agent modeling tool.	Model tested against initial model - verified	Describe terrorist network type
Number of training environments	0 – 100	Increasing training environments also increases radicalism as connection to training	Verified	Simple design of 0-100 training environments to support radicalization training
Information spread intensity / growth (geographic space)	0-100%	Values should generate consistent results, only should occur faster with results	Verified	When considering our attack data – how much information do we have to accurately attack network
Link distance Link connections	0-100 kilometers	Distance (notional kilometers) of support of both radicals and non-radicals alike. Agents with stronger influence should skew total results towards their level of radicalism	Verified	Distance (notional kilometers) of support of both radicals and non-radicals alike
Influence (red/green)	0-100%	Increasing influence values per group generated linear increases in radicalism based on agents level of influence	Parameterize influence of radical leadership vs. non-radical leadership	Parameterize influence of radical leadership vs. non-radical leadership

Network Design

Ronfelt and Arquilla refer to covert organizations, such as terrorist organizations, as having network structures that are distinct from those in typical hierarchical organizations. A key feature of covert networks is that they are cellular and distributed. Understanding how to recognize and attack a terrorist network can be difficult. (Ronfelt and Arquilla, 2001), Therefore the approach of the paper will be to examine multiple network types and examine approaches that are generally consistent in topology, scale, and degree. Given the approach of modeling lone wolf isolationism, networks will model the connectivity between radicals and non-radicals. Low isolation represents a condition where radicals are well-connected to the society at large including many non-radicals. High isolation

represents a condition where the radicals constitute an isolated subnetwork with no or very few ties to non-radicals. High isolation has the greater threat of violence since the radicals experience no restraining influence from non-radicals (Genkin et al, 2011). A suitable measure of isolation is the difference between the number of radical-to-radical ties (internal ties) and radical-to-non- radicals ties (external ties) divided by the total number of ties.

A node for the sake of this model was a single leader within the environment, and as represented by Carley (2008) was also an agent within the model with agent variables. The represented network connections are modeled as a bi-directional graph $G = (N, E)$ consisting of nodes N and edges E. In the context of influence spread, N can be viewed as the users of the social network. Within the model, networks were built dynamically by adding nodes (agents) to locations as specified by the simulation model, and connections were made based on network topology as described below:

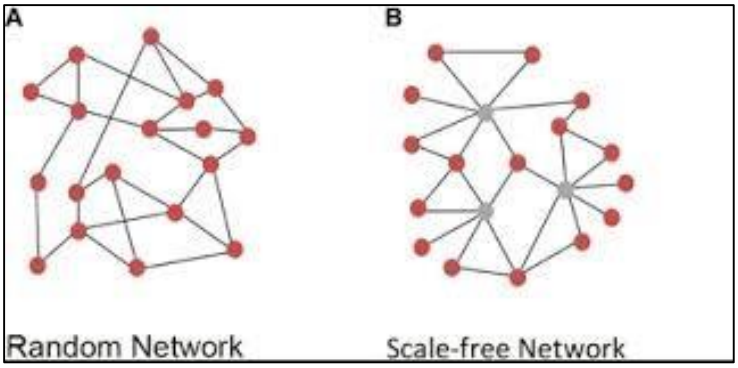


Figure 2: Network Types

Figure 2 shows two types of networks described in the model, random and scale free.

- *The Erdös–Rényi (ER) random network* starts with N nodes and connects each pair of nodes with probability *p*, which creates a graph with approximately *p*N (N-1)/2 randomly placed links (see figure, part **Aa**). The node degrees follow a Poisson distribution (see figure, part **Ab**), which indicates that most nodes have approximately the same number of links (close to the average degree <*k*>).
- *Scale-free networks* are characterized by a power-law degree distribution; the probability that a node has k links follows P(k) ~ k-γ, where γ is the degree exponent. The probability that a node is highly connected is statistically more significant than in a random graph, the network's properties often being determined by a relatively small number of highly connected nodes that are known as hubs.

Developing GIS Space

For the sake of modeling the spread of radicalism, a GIS map[1] (from SAVBAT veg mapping) that mimics the spread of fires in areas that have differences in height and geology. Here my goal is to presume spreading of radicalism is caused both by a) leaders in the area spreading influence and b) geography as a way of illustrating movement over certain types of landscapes. According to Findley, mountainous terrain in an area increases the likelihood of a terrorist connections and forest coverage increases the likelihood of a terrorist attack occurring relative to areas without forest coverage. (Findley, 2015) The rendering in Figure 3 illustrates the spreading of radicalism at varying speeds and distances based on a) the ability to share information through social networks and b) the presense of geographic obstructions and facilitations leading to the physical movement of individuals in the region.

Based on Medina and Hepner's work, I generate a table (see Table 2) illustrating key geographic and virtual terrorist activity spaces. Within my proposed model, each of the four incubation methods described below (havens, training,

[1] https://rohanfisher.wordpress.com/2014/07/12/kimberly-incendiary-sim-netlogo-model/

radicalization, and connection) will be modeled; specifically virtual space methods will be modeled primary through social network representation, and geographic methods through GIS representation, radicalization is modeled through agents and their parameters, and training is modeled as GIS locations that increase radicalization.

Table 2: Courtesy of Medina and Hepner (2013)

Geographic Space		Virtual Space
Exist in places where terrorists are able to live and operate in secure manner	Haven	Terrorists often seek access to safe havens, whether in neighboring countries or hidden in areas
Occurs in places where terrorists train and learn to be 'professional'	Training	Virtual places where terrorists have access to instruction
Occurs physical places where terrorists are exposed to accepting radical ideas	Radicalization	Area where terrorists have access to radical ideas
Occur over networks supporting communication	Connection	Virtual and physical spaces composed of areas of connection (communication)

From here I developed a visualization scheme that provided a semi-realistic depiction of a GIS space with icons that represented additional information within the modelled environment.

Visualization	**Visual Representation**	**Description**
GIS Space	Top-down satellite map	Satellite map of notional high and lowland region including forest and mountainous regions
Networks	Social network graph and connections (gray and white, non-communication and communication respectively)	Network connections simulating information sharing and connections within the simulated environment
Havens	White Houses	Can turn red when radicalization reaches a threshold
Training Areas	Red flag	Area where radicalization tends to grow – connection with traininig areas leads to higher radicalization
Leader Agents	Red (radicalized agents) Gray (neutral agents) Green (non-radical leaders)	Agents appear as 2D icons in geographic space
Population	Black area	Populations are agents within the space that influence spread of radical leaders based on geographic location and level of radicalization in the environment

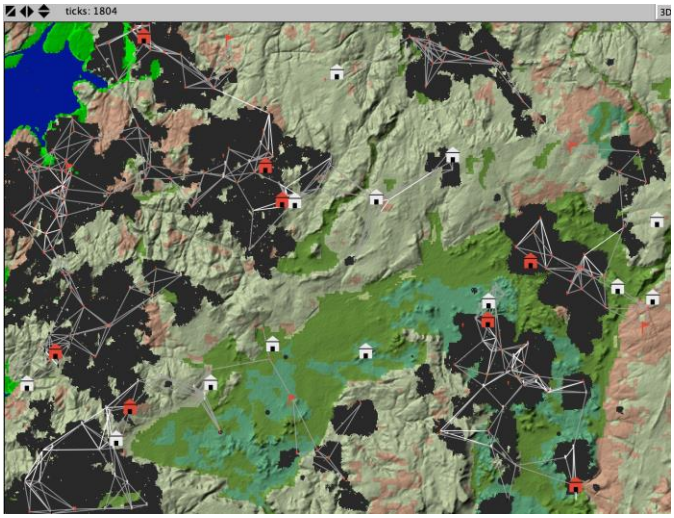


Figure 3: Model GIS Implementation

Temporal Scales

Recent scholars argue that becoming radicalised is, for most people, a gradual process and one that requires a progression through distinct stages and happens neither quickly nor easily (Horgan, 2005; Sibler and Bhatt, 2007). So a person does not become radical overnight, although the influence of an incident which may act as a 'catalyst event'. Ultimately, there are a substantial number of conditions that cause the onset of radicalism, there are no specific rules for time onset other than specific case studies. I shall contain the model to a time at roughly 2.5 years, which is an average time for radicalism to emerge based on several documented examples below. Within the model one tick is equivalent to 24 hours and each simulation run modeled 1000 ticks per session timeframe.

Known growth of radicalism case study	Discussion	Years
2004 MADRID Attack	In mid-2002, some of the main co-coordinators of the attacks began holding their radical discussions in the living room of Faisal Allouch's nearby private house, where they discussed jihad	2002-2004
2006 Ontario terrorism plot	Gravitating Towards Salafi Islam. Similar to the many of those involved in the other plots and attacks, the Toronto plotters also struggled with their identity as evidenced by this excerpt from a poem that was posted on the Internet by Zakaria Amara in 2001.	2001-2006
Hofstad Network	Shortly after the murder of Theo van Gogh by Mohammed Bouyeri in November 2004 the organization gained attention from national media when an attempt to arrest suspected members Jason Walters and Ismail Akhnikh led to a 14-hour siege of a house in The Hague	2001-2004
Virginia Jihad Network	On June 27, 2003, eight of the eleven men were arrested on charges they formed a ``Virginia jihad network'' with ties to the Kashmiri separatist group LeT. 95	2001-2003

Agent Representation using Dynamic Social Network Analysis

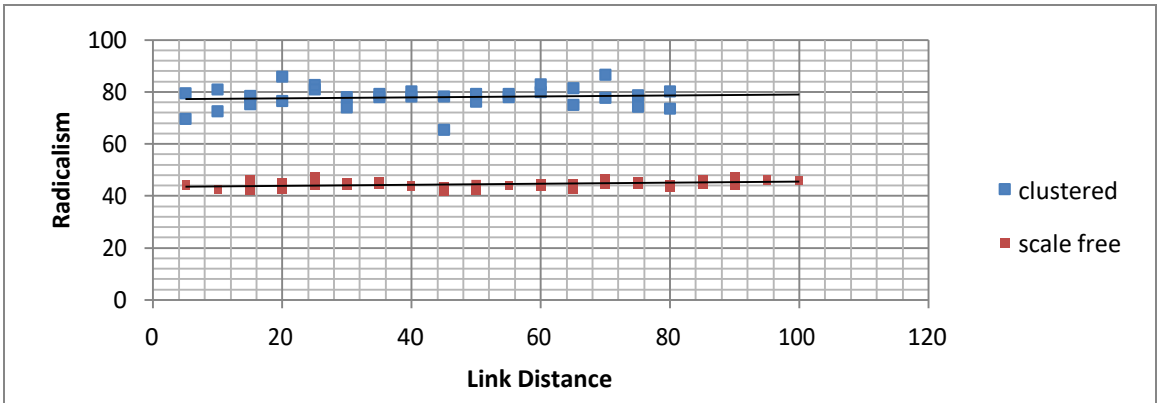
Within my model, I examine the flow of information within a social network model. Carley notes traditional SNA is inadequate in that it only considers the linkage among people, is concerned with non-adaptive systems, and most measures have been tested only for small (< 300 node) networks (Carley, 2003). On the other hand, multi-agent modeling uses very simple unrealistic agents ultimately are not concerned with social network theory, although the systems do adapt. Similar to Carley, the paper proposes a dynamic network analysis model where nodes contain attributes that are representative of terror cells, civilians, and or a hybrid; each having potential desire to inflict terrorist activity on its population.

Terrorist networks are represented as social networks with one of two topologies (small world or clustered network) where nodes represent either a terror cell or an incubation area, and edges represent communication between nodes. In the model used, the amount of communication in the network is interpreted as the total amount of information shared between all nodes in the network. This model was developed in a modern agent based modeling tool with extensions to support both GIS and social network analysis. GIS extends the existing social network model to a social/geospatial model.

RESULTS

In order to identify the most sensitive social parameters for each radicalization scenario, I generated parameter sweeps of each specified value represented in Table 1: Simulation Parameters and verified conditions across consistent parameters. Results are presented in the tables below. To measure the effect of radicalization across network types, I conducted a sensitivity analysis by comparing two distributions: distribution D' for the values of network type 1 (e.g. random clustered), and distribution D (scale free networks). Results were run through an analysis of variance test to determine if results produced two unique data populations. Due to the general complexity of the model I chose to make the key dependent variable in the model *Spread of Radicalism*, where all parameters and actions within the network is evaluated on how they affect this variable.

Network Link Distance: The first parameter, network link distance, yielded a method to minimize network connections to physically close agents. Here subgroups are formed which, to a large extent, share information with similar agent types. The key to distance is that agents of similar breed tend to emerge and cohabitate near one another. Here there is an assumption that agents that are like-minded (homophily) would tend to bolster each other's radical beliefs and could make for a deeper connection to said beliefs. As the agents come into contact with other agents with potential differing beliefs, their bolstered radicalism would not yield to new information.

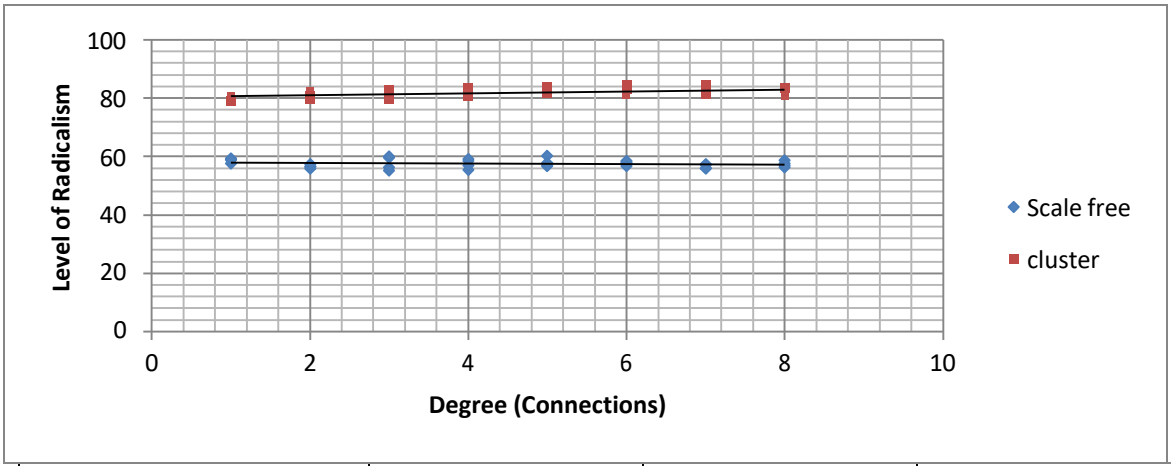


Sample Mean2	Sample Mean	Sample Std.Dev.	R^2
Clustered	55.10624332	4.066874743	.0127
Scale-free	54.94306761	3.411139049	.1676
Sample F statistic	0.075601753		
Critical F statistic	3.900988696		
Degrees Freedom	1		

Decision Rule:	Different populations		
p-value of Sample F:	0.783707931		

Figure 4: Radicalism based on connection distance

Degree (Connections) within Network: I reviewed the notion of degree or number of connections per node. The full picture of radicalization requires more than single radical-to-radical dyad, i.e. more than two individuals, to form an effective cell. For the sake of social network theory I use the concept of cliques that represent agent connections where the clique is a set of nodes that are within a specified distance, are connected with a specified degree, and are not connected to any other group in the simulation. Cliques change in size over time, sometimes over very short periods as more than one clique form into a single unit.



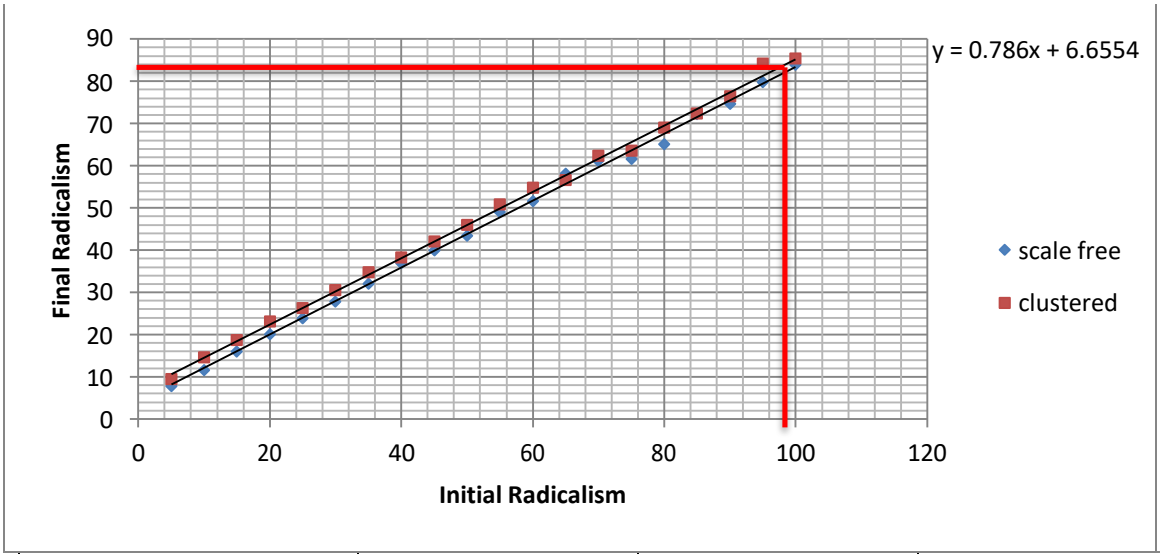
Sample Mean	Sample Mean	Sample Std.Dev.	R^2
Clustered	57.5918683	1.338208476	.27
Scale-free	81.82775695	1.407578917	.1676
Sample F statistic	0	0.075601753	
0	0		
Degrees Freedom	254		
p-value of Sample F:	2.3704E-243		
Decision Rule:	Different Populations		

Figure 5: Radicalism based on number of connections

Sample Mean2	**Sample Mean**	**Sample Std.Dev.**	R^2
Clustered	55.10624332	4.066874743	.0127
Scale-free	54.94306761	3.411139049	.1676
Sample F statistic	0.075601753		
Critical F statistic	3.900988696		
Degrees Freedom	1		
Decision Rule:	Different populations		
p-value of Sample F:	0.783707931		

Interestingly neither factor proved compelling towards affecting the growth of radicalism in either network topology. Both Figure 4 and Figure 5 illustrate that each parameter had weak correlations to the growth of radicalism. I then turned my attention towards what can be termed importance of initial radicalization. What if the initial environment was more radicalization prone? In this context, each agent that has a proclivity towards radicalism begins with a value close to .90 and each non-radical agent begins with a value closer to .25. The results provide some interesting insights, noting that there appears to be a firm correlation overall between initial radicalism and continued level of radicalism within the simulation. On the societal level one can think of this as the propensity to stand relatively firm in beliefs during periods of increasing stress within a societal configuration. So when minimal strain is put on the society (minimal radicalization).

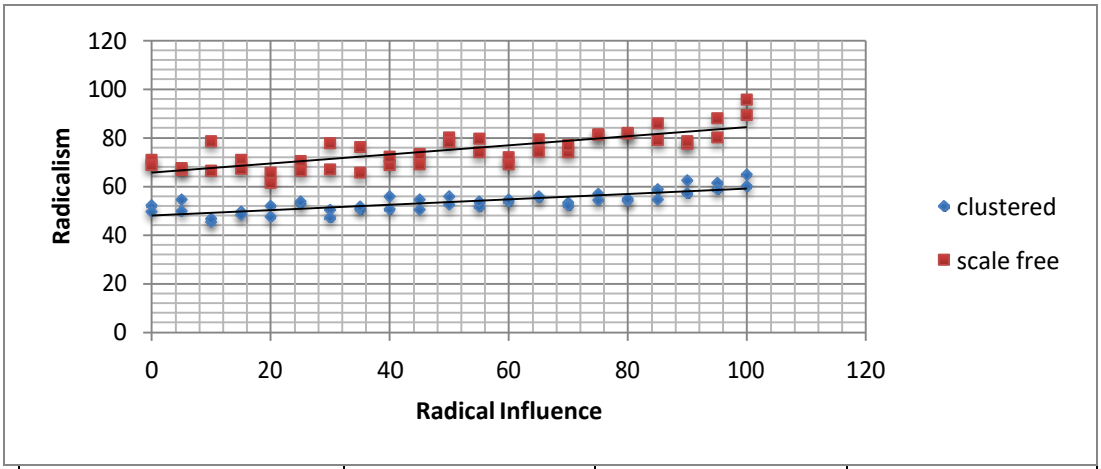
Initial Radicalism: This might be deemed a decreasing returns effect on the population of radicals. Although it appears that there is a strong correlation between the initial level of radicalism in the society and final levels. Although, low doses of radicalism within the society will tend to stay that way over time, while potentially growing due to other factors. But if radicalism begins high, it may be hard to sustain this level over time, possibly due to factors that disrupt networks including alternate anti-radicalism communication. The graph below shows a slowing factor of radicalism with higher initial doses (note the line slopes are > .5)



Sample Mean	Sample Mean	Sample Std.Dev.	R^2
Clustered	45.76166008	23.01859846	.99804
Scale-free	47.91909139	22.82613904	.9978
Sample F statistic	0.354329492	0.075601753	
Degrees Freedom	1		
Decision Rule:	Same Population		
0	0		

Figure 6: Initial radicalism in simulation

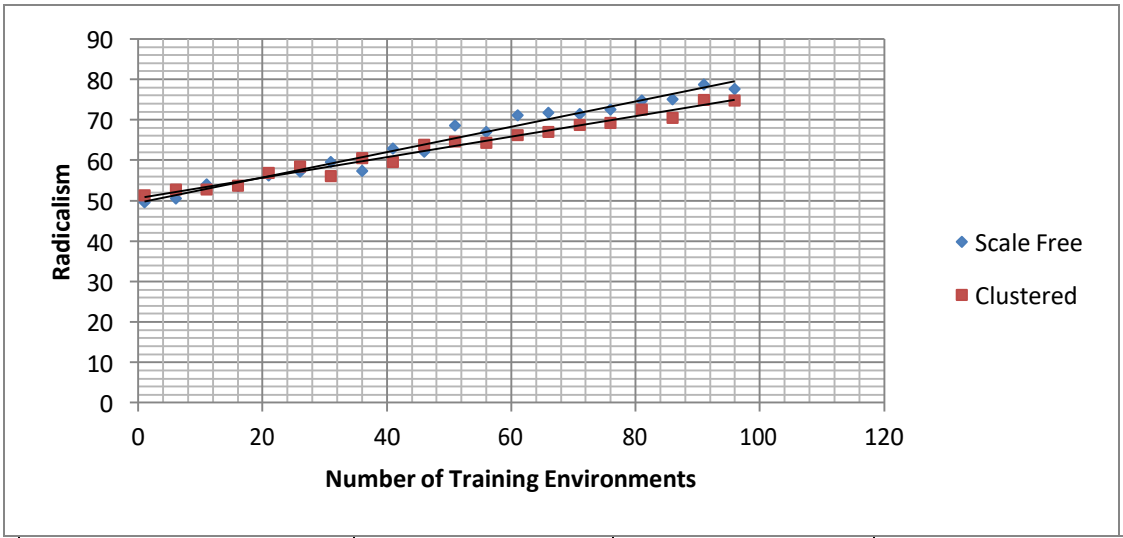
Radical Influence: Within the model there are two influence values, one for radicals and the other for non-radicals. When I ran a parameter space evaluation, I observed that increasing radical influence values for radicals increased the level of radicalism although not with a high degree of correlation. Wiktorowicz (2004) puts greater stress on the role that social influence plays in leading a person to join a radicalised Islamic group. He also states these factors are only believed to be potent during initial onset, with group influences taking over once a person moves towards belonging to a terrorist group (i.e. group dynamics, ideological control, leadership influences, etc).



Sample Mean	Sample Mean	Sample Std.Dev.	R^2
Clustered	53.68094206	4.23625191	.6123
Scale-free	75.03851645	7.378723209	.6305
Sample F statistic	264.6465589	0.075601753	
Critical F statistic	3.957388322		
Degrees Freedom	1		
Decision Rule:	Different Populations		
p-value of Sample F:	2.14653E-27		

Figure 7: Increasing influence

Havens and Training Environments: Another observation illustrating influencing variables within the model is the increase in number of training environments and havens. I reiterate that training environments, akin to their own agent types, act as radical influencers. In modeling terms, agents connect to these havens the way they would any other agent, but these agent links provide a higher degree of both influence and radicalism thereby feeding radical tendencies to all who connect with them. Not unlikely then is that radicalism increases with the number of havens.

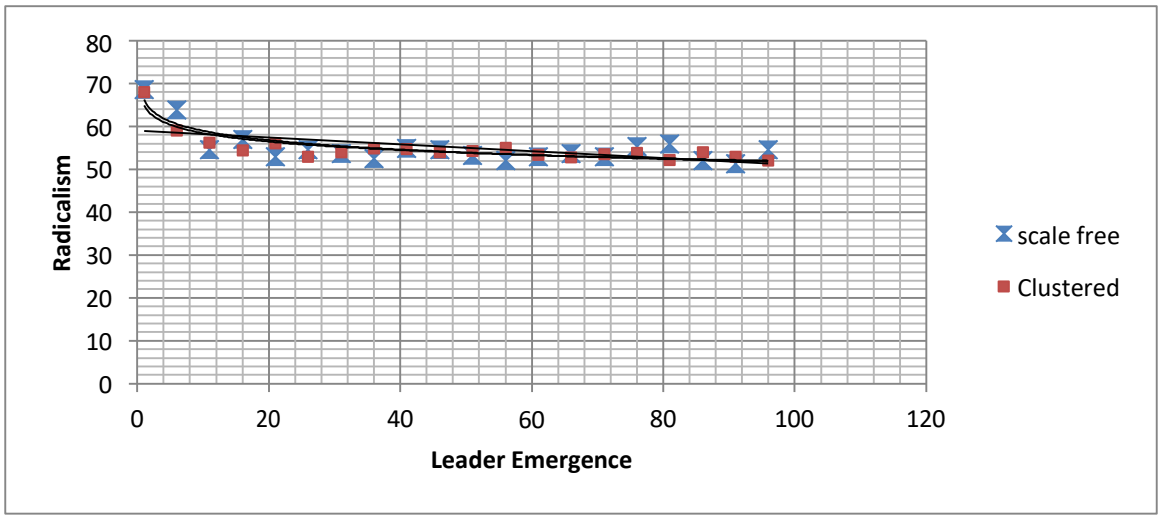


Sample Mean	Sample Mean	Sample Std.Dev.	R^2
Clustered	64.61303002	9.212391548	.97383
Scale-free	62.95427322	7.41809963	.97768
Sample F statistic	1.573435731	0.075601753	
Critical F statistic	3.900988696		

Degrees Freedom	1		
Decision Rule:	Same Population		
p-value of Sample F:	0.21156126		

Figure 8: Increasing havens/training environments

Emergence of Radical Leadership: Lastly I evaluated the role that radical leader emergence played on the spread of radicalism, roughly defined as the time in between the creation of new leadership when radical leadership is ripe for a new purveyor of the cause. Our ANOVA results do show that populations are considered coming from the same sample that may imply that leader emergence is independent of network topology.



Sample Mean	Sample Mean	Sample Std.Dev.	R^2
Clustered	55.10624332	4.066874743	.321
Scale-free	54.94306761	3.411139049	.83412
Sample F statistic	0.075601753	0.075601753	
Critical F statistic	3.900988696		
Degrees Freedom	1		
Decision Rule:	Same Population		
p-value of Sample F:	0.783707931		

Figure 9: Leader emergence probability

DISCUSSION

The paper proposed and analyzed a modest agent-based model based in empirical practices that observed radicalization as a hybrid problem of geo-physical spaces, agent modeling and social network spaces. It presented methods that attempted to validate certain factors such as types of network connections (number of connections, type of networks) and the presence of certain kinds of meeting sites facilitate de/radicalization, while other plausible factors such as community size have little effect. There are several contributes that are brought to bear within the paper. First, are there generizable characteristics that can explain radical influence in a society? I return to the 'lone wolf' isolationism theory where high isolation represents a condition where the radicals constitute an isolated subnetwork with no or very few ties to non-radicals. What would be expected in this case is that high isolated but connected subgroups could in fact gain momentum through mobilizing the story, i.e. radical isolationism could spread through small but agreeable subgroups sharing the common message. Additionally areas or havens that support radical thinking could put additional fuel on the fire through further isolating the subgroup from outside influence, while maximizing radicalization rhetoric.

So how in fact does radicalism grow beyond it's semi-isolationist bounds, and lead to what is termed 'self starter terrorism'? First, we must understand the nature of information sharing in a network subgroup. As even small subgroups share information, the probability of information spread in the proposed model is a conditional probability problem based on *Parallelized Complexity*. Specifically, information spread will often not be enough to restrict information spread, simply because the message (albeit shared by a small group) is not necessarily contained by a single individual. The probability of social complexity by disjunction is given by the following equation, otherwise defined as the logical disjunctive principle:

$$\Pr(Cz) = \Pr(\mathrm{V}Z_{\mathrm{J}}) = 1 - \prod_{\mathrm{j}=1}^{\mathrm{m}} [(1 - \Pr(Z_{\mathrm{QJ}})]$$

The disjunctive mathematical principle is relevant because more than one node may contain relevant information, and removing one will not necessarily disrupt the spread of key information in the network. If we were to compare that to the Conjunctive Principle of Social Complexity defined as the product of probabilities of its n necessary events. Within this theorem, all information flow is linear and non-parallelized. i.e. the decrease in probability of a single event occurring will decrease the probability of the entire event occurring. Therefore, if an event that relied on specific individuals to carry out a task with some probability, the value of one of those events not occurring could substantially jeopardize the likelihood of success.

Although the concept is simple, it is profound. Network types (not necessarily linkages) can play an important part in understanding how radicalism spreads, and can be equally important when trying to destabilize or destroy a network. As Carley (2003) discusses, covert organizations, such as terrorist organizations, tend to be more cellular and distributed, which makes it difficult to apply the lessons of experience in determining how best to destabilize these groups. This problem is further compounded by the vast quantities of, yet incomplete, information. Future models may evaluate influences as to what they know and so what they can do and what organizations they join.
But there are some compelling insights into the understanding of strategies for disrupting networks. Albert, Jeong, and Barabási (2000) published a paper on attack tolerance of complex networks that serves as the basis for most research on scale-free and small-world network attacks. They discovered that scale-free networks can sustain a much higher level of random node removals, but that the networks quickly degrade when the most connected nodes or hubs are removed. Later research quantified this destruction figure at 15% of the most connected nodes to cause network collapse while remaining efficient despite the loss of 80% of nodes in undirected attacks. The implications of this research for terrorism studies is that unless the key leaders within a radical network can be identified, the network can be quite difficult to disrupt. And the problem becomes much more difficult when network connections are more evenly distributed. Future work may include additional statistical validation of the model to include more robust parameter sensitivity evaluation and more advanced cognitive agent representation.

REFERENCES

1. Albert, Réka, Hawoong Jeong, and Albert-Lásló Barabási. (2000) "Error and Attack Tolerance of Complex Networks." Nature 406, No. 6794: 378-382.Ashman, D., Brown, L.D., Zwick, E., (1998) T*he Strength of Strong and Weak Ties: Building Social Capital for the Formation and Governance of Civil Society Resource Organizations* IDR Reports, Volume 14.2
2. Arquilla, J. and Ronfeldt, D (2001) Networks and Netwars: The Future of Terror, Crime, and Militancy(eds). RAND: National Defense Research Institute
3. Bak, P., 1996. How Nature Works: The Science of Self-Organized Criticality, Copernicus.
4. Barabási, A. L. (2002). Linked: The new science of networks. Cambridge, Massachusetts: Perseus Publishing.
5. Berman, E., Shapiro, J. (2011), Can Hearts and Minds be Bought? The Economics of Counterinsurgency in Iraq, Journal of Political Economy 119(4), 766-819
6. Borgatti, S.P., (2002), "The Key Player Problem," Proceedings from National Academy of Sciences Workshop on Terrorism, Washington DC.

7. Butts, Carter T. (2003a). ―Network Inference, Error, and Informant (In) Accuracy: A Bayesian Approach‖, Social Networks 25(2) 103-30.
8. Butts, Carter T. (2003). "Predictability of Large-scale Spatially Embedded Networks." In Ronald Breiger, Kathleen Carley, and Philippa Pattison (eds.), Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, 313-323. Washington, D.C.: National Academies Press. Royal Society International Centre, Newport Pagnell, UK, 24–25 September 2012
9. Carley, Kathleen (2003). "Destabilizing Terrorist Networks." Proceedings of the 8th International Command and Control Research and Technology Symposium. National Defense War College, Washington DC.
10. Carley, K.M. (1997). Network Text Analysis: the network position of concepts. In Carl W. Roberts (Ed.), Text analysis for the social sciences, (pp. 79-102). Mahwah, NJ: Lawrence Erlbaum Associates.
11. Cioffi-Revilla, Claudio (2013). Introduction to Computational Social Science: Principles and Applications (Texts in Computer Science) (Kindle Locations 5631-5635). Springer London. Kindle Edition. Crawford, Vincent P., Sobel, Joel, (NDG) *Strategic Information Transmission*, Econometrica Vol. 50, No. 6 , pp. 1431-1451 Published by: The Econometric Society
12. Fellman, P.V. (2011). Understanding the Complexity of Terrorist Networks: Ref Unknown
13. Hoffman, Bruce (1997) ―The Modern Terrorist Mindset: Tactics, Targets and Technologies‖, Centre for the Study of Terrorism and Political Violence, St. Andrews University, Scotland, October, 1997
14. Hoffman, Bruce and Carr, Caleb (1997) , Terrorism: Who Is Fighting Whom?" World Policy Journal, Vol. 14, No. 1, Spring 1997
15. Holland, J.H. (1995), Hidden order. How adaptation builds complexity. Reading: Addison Wesley Kauffman publishing company.
16. Kauffman, S.A. (1995) At home in the Universe, Oxford: Oxford University Press.
17. Martonosi, S.E., and D.S. Altner. (2009). RUI: Collective research: Algorithms for threat detection: Detecting clandestine members of covert net- works. NSF Grant Proposal.
18. Krackhardt, David, and Robert N. Stern. (1988). Informal networks and organizational crises : An experimental simulation. Ithaca, NY: Cornell University ILR Press.
19. Medina, R. and Hepner, G (2013) The Geography of International Terrorism, An Introduction to Spaces and Places of Violent Non-state Groups," Taylor and Francis/ CRC, pp. 258
20. Medina, R., Siebeneck, L., Hepner, G. (2011), A Geographic Information Systems (GIS) Analysis of Spatiotemporal Patterns of Terrorist Incidents in Iraq 2004–2009, Studies in Conflict & Terrorism, 34:862–882, 2011 Copyright © Taylor & Francis Group, LLC
21. Reid, E. Quin, J. Chung, W. (2004), Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach to Address the Threats of Terrorism, (Working paper).
22. Sageman, M.(2004), Understanding Terror Networks (Philadelphia: University of Pennsylvania Press,)
23. Taspınar, Omer (2009) Fighting Radicalism, not 'Terrorism': Root Causes of an International Actor Redefined, SAIS Review International vol. XXIX no. 2 (Summer–Fall 2009)
24. Tsvetovat, Max & Carley, Kathleen. (2003). Bouncing Back: Recovery mechanisms of covert networks. NAACSOS Conference 2003