Destabilizing Terrorist Networks

Kathleen M. Carley
Jeffrey Reminga
Natasha Kamneva
Carnegie Mellon University

Contact:
Prof. Kathleen M. Carley
Institute for Software Research International
Carnegie Mellon University
Pittsburgh, PA 15213

Tel: 1-412-268-6016
Fax: 1-412-268-1744
Email: kathleen.carley@cmu.edu

Modeling and Simulation

This paper is part of the Dynamics Networks project in CASOS at CMU. This work was supported in part by the Office of Naval Research (ONR), United States Navy Grant No. 9620.1.1140071 on Dynamic Network Analysis under the direction of Rebecca Goolsby and Grant No. 1681.12.1140053 on Adaptive Architecture under the direction of Bill Vaughn. Additional support on measures was provided under the Darpa project on INSIGHT (Interpreting Network Structures to obtain Intelligence on Groups of Hidden Terrorists) DAAH01-03-C-R111. Additional support was provided by NSF Igert program and CASOS – the center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University (http://www.casos.ece.cmu.edu). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research, Darpa, the National Science Foundation or the U.S. government. Many thanks to Connie Fournelle and ALPHATECH for providing data and comments.

Destabilizing Terrorist Networks

Abstract:

Most people have at least an intuitive understanding of hierarchies, how they work, and how to affect their behavior. However, covert organizations, such as terrorist organizations, have network structures that are distinct from those in typical hierarchical organizations. Their structure is distinct from the organizations that most people in western culture are used to dealing with. In particular, they tend to be more cellular and distributed. As such, most people do not have an intuitive understanding of how they work and instead seek to think of them as hierarchies. However, analysis reveals that trying to destabilize a cellular distributed network using tactics designed for hierarchies is likely to be ineffective. A secondary problem is that despite the vast quantities of information on the size, shape and structure of these networks, such, information is incomplete and possible erroneous. What is needed is a set of tools and an approach to assessing destabilization strategies in a decision context that takes these difficulties in to account and provides analysts with guidance in assessing alternative destabilization tactics. Such an approach is forwarded in this paper. In addition, initial lessons learned are discussed. The particular approach is extensible and scales well to groups composed of 1000's of members.

Support: This research has been supported, in part, by the National Science Foundation IGERT in CASOS, the Office of Naval Research (ONR), United States Navy Grant No. 9620.1.1140071 on Dynamic Network Analysis and Grant No. 1681.12.1140053 on Adaptive Architecture, DARPA, the NSF under the IGERT award in CASOS - NSF IGERT 9972762, and the center for Computational Analysis of Social and Organizational Systems. The views and results expressed herein are solely the responsibility of the authors and do not represent the official views of the Office of Naval Research, DARPA or the National Science Foundation.

Approaches to Assessing Destabilization Tactics for Dynamic Networks

Most people have at least an intuitive understanding of hierarchies and how to affect their behavior. However, covert organizations, such as terrorist organizations, have network structures that are distinct from those in typical hierarchical organizations. A key feature of covert networks is that they are cellular and distributed. Consequently, the lessons of experience held by these decision makers may not be applicable. Reasoning about how to attack dynamic networked organizations (Ronfelt and Arquilla, 2001), let alone figuring out how they are likely to evolve, change, and adapt is terribly difficult. What is needed is a series of tools, techniques, and models for collecting data on and reasoning about these covert networks even in the face of overwhelmingly incomplete information.

To understand the dynamics of covert networks, and indeed any, network we need to understand the basic processes by which networks evolve. Moreover, we have to evaluate destabilization and surveillance strategies in the face of an evolving network and in the face of missing information. To ignore either the dynamics or the lack of information is liable to lead to erroneous, and possibly devastatingly wrong, policies. Taking in to account both the dynamics and the lack of information should engender a more informed approach to answering various policy questions. Key questions might include "what is the size and shape of the covert network", "how does the nation in which the covert network exists impact its form and ability," and "if we do x to the covert network what is likely to happen?"

Two approaches that could be applied to the study of covert networks are traditional social network analysis and multi-agent modeling (particularly a-life). However, both of these approaches are severely limited. Traditional SNA is limited 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. Multi-agent modeling uses very simple unrealistic agents who, although they adapt, move about only on a grid and don't take actual networks in to account. This paper proposes the use of a third approach – dynamic network analysis.

Approaches to Assessment

Dynamic Network Analysis (DNA) extends the power of thinking about networks to the realm of large scale, dynamic systems with multiple co-evolving networks under conditions of information uncertainty with cognitively realistic agents (Carley, 2002b). DNA has been made possible due to three key advances: 1) the meta-matrix (Carley, 2002a; Krackhardt and Carley, 1008) connecting various entities such as agents, knowledge and events, 2) treating ties as "variable" and so having a weight and/or probability, and 3) combining social networks with cognitive science and multi-agent systems to endow the agents with the ability to adapt (Carley, 2002c). In a meta-matrix perspective a set of networks connecting various entities such as people, groups, knowledge, resources, events, or tasks are combined to describe and predict system behavior. In variable tie perspective, connections between entities are seen as ranging in their likelihood, strength, and direction rather than as being simple binary connections indicating exclusively whether or not there is a connection. Finally, the utilization of multi-agent network models enables the user to reason about the dynamics of complex adaptive systems. In particular, these computational models combine our understanding of human cognition, biology, knowledge management, artificial intelligence, organization theory and geographical factors into a comprehensive system for reasoning about the complexities of social behavior.

A key feature underlying this work is a dynamic approach to the co-evolution of agents, knowledge, tasks, organizations and the set of inter-linked networks that connect these entities. Multi-agent network modeling is used to capture the complexities by which who people know influences what they know and so what they can do and what organizations they join. Changes at each unit of analysis, person to group to organization to society impact changes at the next; however, the rate of change decreases and the size of the change's impact increases as unit size increases. Another feature is that each agent (and indeed each unit) has transactive knowledge – knowledge of who knows who, what, is doing what, and is a member of what. This knowledge is typically incomplete, sparse, and potentially wrong. However, the actions of the agents are based on their perception of the network not the actual network. Cognitive, social, task, and cultural constraints limit what entities are present, what/who can be connected to what/who, when and how those connections can change, when new entities (such as new agents) can be added or old one's dropped, and so on.

Proposed Approach

The basic approach that we use to assess destabilization tactics is the following:

1. Identify key entities and the connections among them.
2. Identify key processes by which entities or connections are added or dropped, or in the case of connections, changed in their strength.
3. Collect data on the system (covert network).
4. Determine performance characteristic of existing system.

5. Determine performance characteristics of possible optimal system.
6. Locate vulnerabilities and select destabilization strategies.
7. Determine performance characteristics in the short and long term after a destabilization strategy has been applied.

Some comments on this approach are warranted. First, the result of this process is an evaluation of both system vulnerabilities and the impact of attacking those spots, with some estimate of the robustness of the results in the case of missing information. By providing both the vulnerabilities and the impact of attack, the analyst can use this information to consider the possible ability of these attacks to effect other outcomes other than the specific performance characteristics examined. Second, the process as described above is very general. We have instantiated at this point, and will describe, a relatively simple form of this process. It is important to note that the approach is broader than this simple instantiation. It is in this sense that we say that the approach is extensible.

We illustrate this instantiation using data collected on an embassy bombing in Tanzania. We refer to this as the embassy bombing data set (EB data set). This data was collected from open source files, such as newspaper reports, by Connie Fournelle at ALPHATECH. The key entities that we have identified are people (agents), knowledge, resources, events, tasks, groups, and countries. For the sake of exposition, and without loss of generality, we utilize a smaller set of entities: people, resources, and tasks. These are identified in table 1.

Table 1. EB data set characteristics

	People	Resources	Tasks
People Number of nodes	Social/authority network 16x16	Capabilities network 16x8	Assignment network 16x5
Resources Number of nodes		Substitution Network 8x8	Needs network 8x5
Tasks Number of nodes			Precedence network 5x5

To measure performance, we take the extant system and simulate it using DyNet. DyNet is a multi-agent network system for assessing destabilization strategies on dynamic networks. DyNet uses the Construct code for assessing information diffusion and accuracy (see for details Carley, 1991, 1999; see also for description of the binary classification task, Carley & Svoboda, 1996). In simulating the system, a knowledge network for the system is given to DyNet as input. We define knowledge here as the individual's knowledge about who they know, what resource they have, and what task they are doing. We make the simplifying assumption that each agent knows about the complete set of available persons, resources and tasks and has no knowledge of what others know. Due to the level of granularity of the data, the alternative assumption that each agent has perfect knowledge of who knows whom, who has what resources, and who is doing what tasks, has little impact on the results.

By identifying the mission and technology constrained portions as relatively fixed components of the extant system linking tasks to tasks and resources, at least in the short run, we open the possibility to locating the optimal form or structure of the rest of the system. We define the organizational design as the set of cells in the meta-matrix that can be varied in the short run – the social networks, the capabilities network, and the assignment network. The system is optimized if the ties in this network are arranged such that they minimize vulnerabilities. We

define a system to have the optimal organizational configuration or design if vulnerabilities due to one or more of the following are minimized: distribution of resources, distribution of communication ties, and workload. Our results suggest that the organization was not particularly efficiently designed and/or there is substantial missing data about the organizational design. The current organizational design requires 88 changes in who is doing what and has what resources in order to reach the optimal configuration. This represents 42% of the 208 possible linkages that could be changed. This indicates that a random change is slightly more likely to destabilize the organization and move it further from the optimum. We now take the original organization and ask, how should it be destabilized?

Four distinct strategies for destabilizing the organization have been identified: eliminate the person with the highest degree centrality, betweenness centrality, cognitive load, or task exclusivity. We measure the impact of isolating the individuals high in these measures in two ways. First, using ORA, we contrast the relative resource congruence of the organizations without the isolated individual. Second, using DyNet, we contrast the relative change in performance in terms of accuracy and diffusion and ability to adapt to this change for the organization with and without these individuals. The results of these removals are shown in table 2. All differences shown are significant. Neither removal substantially moves the design further from the optimal. Hence, we would expect the effects to be small. In addition, the removal of agent 5 actually increases resource congruence over the original design. On first blush, this is not good. However, keep in mind that resource congruence is a strict measure such that congruence is decreased when either agents do not have the resources needed for the task to which they are assigned or when agents have resources that are not necessary for the task that they are assigned. Removal of agent 5 is reducing the presence of unnecessary resources. Thus making the organizational design leaner. Making the organization optimal by reducing redundancy also make the organization less adaptive. Thus the removal of agent 5 makes the organization both more efficient but less adaptive.

If we explore diffusion the opposite is the case. For diffusion, the removal of agent 7 both lowers the initial diffusion more (compared to the removal of no agent) and it slows the rate at which diffusion is possible. Whereas, although the removal of agent 5 does drop the level of diffusion, it actually increases the rate of spread. In this case, the removal of agent 7 is more disruptive to the communication flows. It is important to keep in mind that this is the speed of information flow not the quality. Since the removal of agent 5 actually speeds the rate of information flow, it is speeding both the flow of accurate and inaccurate information. This potentially makes the organization more vulnerable to information warfare attacks.

Table 2. Impact of Agent Removal

Measure	Original Design	After Removal of 5	After Removal of 7
Hamming from Optimal	88	83	86
Resource congruence	.475	.525	.475
Performance as Accuracy – Initial Impact	78.5625	78.22	82.72
Performance Recovery – Percentage Increase in Performance	95.55	89.72	93.7
Diffusion - Initial	21.62291	14.70212	13.27369
Diffusion Recovery – Percentage Increase in Diffusion	71.23304	89.05325	50.87843

Future work should expand on this by considering other criteria for optimization, examining larger organizations where there are more complex networks, and explore other performance outcomes. Moreover, a key concern that needs to be addressed is the flow of incorrect information and the relative impact of such information warfare as opposed to personnel attacks.

References

Borgatti, S.P., 2002, "The Key Player Problem," Proceedings from National Academy of Sciences Workshop on Terrorism, Washington DC.

Carley, Kathleen M. 2002c, "Inhibiting Adaptation" In Proceedings of the 2002 Command and Control Research and Technology Symposium. Conference held in Naval Postgraduate School, Monterey, CA. Evidence Based Research, Vienna, VA.

Carley, Kathleen M. 2002b, "Dynamic Network Analysis" Paper presented at National Academy of Sciences/ National Research Council, Committee on Human Factors, Workshop on Dynamic Social Network Analysis, Washington D.C., November 2002. To be published in proceedings.

Carley, Kathleen M. 2002a, "Smart Agents and Organizations of the Future" The Handbook of New Media. Edited by Leah Lievrouw & Sonia Livingstone, Ch. 12 pp. 206-220, Thousand Oaks, CA, Sage.

Carley, Kathleen M. 1999. "On the Evolution of Social and Organizational Networks." In Vol. 16 special issue of Research in the Sociology of Organizations on "*Networks In and Around Organizations* " edited by Steven B. Andrews and David Knoke. JAI Press, Inc. Stamford, CT, pp. 3-30.

Carley, Kathleen M. & David Krackhardt, 1999, "A Typology for C^2 Measures." *In Proceedings of the 1999 International Symposium on Command and Control Research and Technology*. Conference held in June, Newport,RI., Evidence Based Research, Vienna, VA.

Carley, Kathleen M. 1991. "A Theory of Group Stability." American Sociological Review 56(3): 331-354.

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

Carley, Kathleen M. & David M. Svoboda, 1996, "Modeling Organizational Adaptation as a Simulated Annealing Process." *Sociological Methods and Research*, 25(1): 138-168.

Freeman, L.C., 1979. Centrality in Social Networks I: Conceptual Clarification. Social Networks, 1, 215-239.

Krackhardt, D. and K. Carley, 1998, "A PCANS Model of Structure in Organization," In: *Proceedings of the 1998 International Symposium on Command and Control Research and Technology*, 113-119.

Lin, Zhiang and Kathleen M. Carley, 2003, Designing Stress Resistant Organizations: Computational Theorizing and Crisis Applications, Boston, MA: Kluwer.

Ronfeldt, D. and J. Arquilla. September 21, 2001. "Networks, Netwars, and the Fight for the Future," First Monday, Issue 6 No. 10. online: http://firstmonday.org/issues/issue6_10/ronfeldt/index.htm.