BOUNCING BACK: RECOVERY MECHANISMS OF COVERT NETWORKS

MAKSIM TSVETOVAT AND KATHLEEN M. CARLEY
CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA
MAKSIM@CS.CMU.EDU, KCARLEY@ECE.CMU.EDU

1. Introduction

In study of covert networks and destabilization strategies thereof, much attention has been paid to the task of locating and isolating key individuals within the organization. Metrics such as centrality, betweenness, cognitive load, and others, have all been used for that purpose. The isolation act was considered successful if it resulted in the network being separated into disconnected subparts.

However, the real-world covert networks that have been a target of various isolation strategies have shown a high level of resilience, and were able to quickly recover from the damage caused by the isolation.

In this paper, we show that cellular covert networks use transactive memory and other latent resources as a mechanism for recovery from events that partition the network. Using a multi-agent network simulation, we proceed to show the recovery process and its effects on performance of the cellular network.

2. Nature of Covert Networks

While the history of warfare is mainly represented by conflicts involving conventional armies of approximately equivalent organizational structure and strength, in many cases small, dispersed and seemingly disorganized group shave been able to effectively counter much larger conventional armies. Large terrorist organizations operate in small, dispersed cells that can deploy anytime and anywhere [11].

There are several factors that allow a terrorist organization to remain covert.

- Members sharing strong religious or ideological views that allow them to form extremely strong bonds within a cell, further reinforced by physical proximity, with members of cells sharing living quarters, working and training together.
- Members of cells are hidden from the rest of the organization, and likely do not know much about the organizational structure or even the size of the organization

This work was supported in part by the Office of Naval Research(ONR), United States Navy Grant No.N00014-97-1-0037, NSF IRI9633 662 and the NSF IGERT in CASOS. 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.

- Information about tasks is issued on the need-to-know basis, so very few people within the organization know the operational plans in their entirety.

However, limiting the knowledge to need-to-know basis within the cells is counterproductive when an organization needs to complete a task. To fix this inefficiency, terrorist organizations have been known to employ "sleeper links", such as family ties, ties emerging from common training, etc [10]. These links are rarely activated and used mainly for coordinating actions of multiple cells in preparation for a larger operation.

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 [9]. Terrorist organizations are also characterized by the difficulty in deciding which nodes constitute active parts of the network and which are "innocent bystanders".

The best profile of structure of terrorist networks, based on publicly available data, is the following [6]:

- 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.

3. Destabilization of Covert Networks

Extra-national terrorist networks are known to be fluid in their distribution of resources and personnel, thus making a concentrated assault difficult. The distributed nature of terrorist networks also allows them to keep the resource bases decentralized and difficult to find. Often such bases are located in the midst of civilian life, using the non-combatants as human shields. A concentrated assault on such a base can result in numerous civilian casualties, and result in a PR fiasco for the assaulting party.

A common type of attacks against terrorist networks is isolation of agents, where isolation can mean disabling of communications, arrest or even assassination of the agent. Common targets for isolation are publicly known leaders of the organization, people implicated in previous terrorist acts, and known experts within the organization.

Precise targeting of isolation attacks is extremely important and must take into account the organizational structure, task assignments and performance within the organization and knowledge and resource distribution. This information is commonly referred to as meta-matrix[4][5](see table **??**). The simulation experiments described further in this paper illustrate the value of meta-matrix awareness in isolation and information warfare operations.

4. Covert Networks and Social Network Methods

A number of social networks metrics have been proposed as relevant to the issue of finding emergent leaders of covert networks from sparse intelligence date and using this information to disrupt or destabilize terrorist networks and their command-and-control structures.

The *centrality approach*, consisting of measuring the centrality of each node in the network, then selecting a small number of most central nodes as targets for further action, is an intuitive approach to finding a core group of leaders within a terrorist network. However, from available intelligence it is known that terrorist networks function in tightly connected cells and maintain only loose connections with the rest of the organization. Therefore, a search for highly central individuals is more likely to turn up a large number of agents that do not constitute the leadership circle, but are members of a densely connected cell. Moreover, as Borgatti [2] stated, none of the centrality metrics is guaranteed to disconnect the network into discreet components.

Bienenstock and Bonacich [8] have conducted a simulation study on vulnerability of networks to random and strategic attacks. The study suggests that as averatge connectedness of each individual node rises and high betweenness nodes are methodically attacked, the impact on overall performance of the network is minimal. However, if neighborhoods (nodes connected to a high-centrality node) are attacked along with the node, the opposite is true. The implication of that result is that the cells of covert networks that are connected by a few individuals with high betweenness are very vulnerable to discovery of these individuals.

Other graph theoretic approaches to finding critical nodes in covert networks concentrate on the notion of cutpoints and bridges, which are nodes and lines, respectively, whose deletion would increase the number of components in the graph. For the purpose of destabilizing terrorist networks, the optimization problem of minimum weight cutsets can be inverted to maximize the number of components into which a graph is separated, for a given size of cutset.

The *cognitive load* approach described by Carley [7], combines static measures of centrality with dynamic measures of information flow, task performance and resource distribution. These measures are based on the meta-matrix knowledge about the organization and have been shown to accurately detect emergent leaders. Consequently, cognitive load metrics can potentially be useful for detecting key members of terrorist networks.

Other metrics of node criticality, such as *knowledge* and *task exclusivity* [1] are heralded as able to most accurately detect key individual in covert networks. However, they remain largely untested.

5. NetWatch: Multi-Agent Network Simulation of Covert Networks

To address the problems in studying covert networks that were illustrated above, we have designed NetWatch - a multi-agent network model of covert networks and anti-terrorist activity

NetWatch is designed to:

- simulate the communication patterns, information and resource flows in a dynamic covert cellular network;

- model the process of gathering signal intelligence on a cellular network and evaluate a variety of heuristics for ingelligence gathering;
- model and evaluate strategies for destabilizing a covert network based on intelligence obtained;
- model reactions of a covert network to these destabilization strategies.

The cognitive underpinnings of the covert network model are based upon the CONSTRUCT information diffusion model [4][3]. The agents in the model perform a classification task that is information-intensive. Agents learn by interaction with other agents in process of completing the task.

The simulation consists of several networks of agents: the **Red Team**, representing the covert network of a terrorist organization, the **Blue Team** representing the anti-terrorist or law enforcement forces, and a set of instrumentation agents that observe and document the behaviour of other agents for later retrieval and processing.

The Red Team, or the Covert Network consists of a set of small fully-interconnected cells of agents with little interconnect between them, mimicking the organizational structure of a terrorist organization.

The Blue Team is an Anti-Terrorism organization consisting of a small number of fully interconnected law enforcement agents. The goals of the Blue Team are to learn as much as possible about the meta-matrix structure of the Red Team and use knowledge obtained to remove or isolate Red Team members, aiming to impair Red Team's performance.

6. Recovery Mechanisms of Covert Networks

A priority in research on destabilization of covert networks has been finding key individuals removal of which will separate a cellular network into subparts. However, our experiments have shown that after a covert networks is separated into disconnected cells, the network will use its latent resources and quickly recover from damage.

The process of recovery is based on use of referential data to contact members of other cells bypassing a gatekeeper. However, in order for such connection to succeed, the referential data must be mutual - both parties of the conversation have to have referential knowledge of each other.

Such occurrences are fairly rare due to the very function of a gatekeeper, which insulates cells from each other by filtering information that passes through it. If the gatekeeper filters out 70% of referential data, the probability of successful connection between any two agents is $< 10\%$.

Cell reconnection attempts fail (in approximately 32% of cases in our simulation) if no pair of agents finds mutual referential data on each other. In this case, the effect of disconnection on performance of the covert network depends on whether the newly disconnected cell possessed information or resources that were otherwise scarce in the organization. If the cell was close to self-sufficiency, it will continue to operate on its own. Otherwise, the cell will fall dormant until a new source of resources is found.

If one reconnection attempt succeeds, the agents will find that the newly connected pair of agents is the lowest-cost communication path to the neighboring cells (as cost is measured in number of attempts required to get a message across), and thus use them as a conduit for external communication. The initiator of the

successful connection will, thus, emerge as a new gatekeeper separating the two cells.

In about 5% of remaining cases, two or more reconnection attempts succeed simultaneously. This results in creation of multiple redundant paths between cells. This essentially results in one cell being absorbed in another. The combined cells function well on tasks that do not require much interaction, but the overhead of extra connection drives down performance on deliberation- intensive tasks.

7. Discussion

The goal of anti-terrorist activity should be to cause permanent damage to the covert networks and not allow it to recover from the attack. However, we found through our simulation study that covert networks quickly recover from removal of gatekeepers and agents with high cognitive load by use of referential data.

This finding stresses the importance of studying covert networks as dynamic systems, and evaluating effect of destabilization techniques on performance through realistically modelled tasks instead of abstract measures such as number of components.

References

1. Michael Ashworth and Kathleen M. Carley, *Identifying critical human capital in organizations*, CASOS Working Paper, 2002.
2. Stephen Borgatti, *The key player problem*, Proceedings of CASOS 2002 Conference (Pittsburgh, PA), 2002.
3. Kathleen M. Carley, *A theory of group stability*, American Sociological Review **56** (1991), no. 3, 331–354.
4. _____, *On the evolution of social and organizational networks.*, Research in the Sociology of Organizations **16** (1999), no. special issue on Networks In and Around Organizations, 3–30.
5. _____, *Smart agents and organizations of the future*, The Handbook of New Media (Leah Lievrouw and Sonia Livingstone, ed.), Sage, Thousand Oaks, CA, 2002, pp. 206–220.
6. Kathleen M. Carley, Ju-Sung Lee, and David Krackhardt, *Destabilizing networks*, Connections **24** (2001), no. 3, 31–34.
7. Kathleen M. Carley and Yuquing Ren, *Tradeoffs between performance and adaptability for c3i architectures*, Proceedings of the 2000 International Symposium on Command and Control Research and Technology (2001).
8. E.J.Bienenstock and P. Bonacich, *Balancing efficiency and vulnerability in social networks*, Summary of the NRC workshop on Social Network Modeling and Analysis (Ron Breiger and Kathleen M. Carley, eds.), National Research Council, forthcoming.
9. Bonnie H. Erickson, *Secret societies and social structure*, Social Forces **60** (1981), no. 1, 188–210.
10. Valdis E. Krebs, *Mapping networks of terrorist cells*, Connections **24** (2001), no. 3, 43–52.
11. D. Ronfeldt and J. Arquilla, *Networks, netwars and the fight for the future*, First Monday **6**, no. 10.