CentER

Discussion Paper

No. 2008–23

THE INFLUENCE OF SECRECY ON THE COMMUNICATION STRUCTURE OF COVERT NETWORKS

By Roy Lindelauf, Peter Borm, Herbert Hamers

February 2008

ISSN 0924-7815

TILBURG UNIVERSITY

The Influence of Secrecy on the Communication Structure of Covert Networks

Roy Lindelauf [a,b,c] Peter Borm [b] Herbert Hamers [b]

February 2008

[a]Military Operational Art & Science, Netherlands Defense Academy, P.O.Box 90002, 4800 PA Breda, The Netherlands. E-mail: rha.lindelauf.01@nlda.nl

[b]CentER and Department of Econometrics and OR, Tilburg University, P.O.Box 90153, 5000 LE Tilburg, The Netherlands.

[c]Corresponding author

The Influence of Secrecy on the Communication Structure of Covert Networks

Abstract

In order to be able to devise successful strategies for destabilizing terrorist organizations it is vital to recognize and understand their structural properties. This paper deals with the optimal communication structure of terrorist organizations when considering the tradeoff between secrecy and operational efficiency. We use elements from game theory and graph theory to determine the 'optimal' communication structure a covert network should adopt. Every covert organization faces the constant dilemma of staying secret and ensuring the necessary coordination between its members. For several different secrecy and information scenarios this dilemma is modeled as a game theoretic bargaining problem over the set of connected graphs of given order. Assuming uniform exposure probability of individuals in the network we show that the Nash bargaining solution corresponds to either a network with a central individual (the star graph) or an all-to-all network (the complete graph) depending on the link detection probability, which is the probability that communication between individuals will be detected. If the probability that an individual is exposed as member of the network depends on the information hierarchy determined by the structure of the graph, the Nash bargaining solution corresponds to cellular-like networks.

Keywords: covert networks, terrorist networks, Nash bargaining, game theory, information, secrecy.

JEL classification: C50, C78.

1 Introduction

Terrorist networks inside the Western world pose a challenge to the security environment (Vermaat 2002). Furthermore it is known that Europe is a key staging ground for jihadi activities (Vidino 2007). These terrorist organizations are often characterized as cellular organizations composed of quasi-independent cells and distributed command (Tsvetovat 2005). In addition they are characterized as being organized decentralized rather than hierarchical (Tucker 2001). It is also recognized that there are terrorist organizations that operate according to organizational structures that lie somewhere between hierarchical and completely decentralized (Mishal 2005). Terrorist organizations are aware of the importance of their network structure and take this explicitly into account when conducting operations: in a video lecture captured after the fall of Afghanistan in 2001 Mousab al Suri (aka Mustafa Nasar the Syrian, an alleged Al Qaeda affiliate) discusses the structure a covert organization should adopt (Bergen 2006). He indicates that certain network structures should be avoided to ensure the secrecy of the organization. Similar considerations are taken into account in the field of military swarming. Here units resemble an array of dispersed nodes set to act as an all-channel network. The challenge is to design military networks that depend on stealth and secrecy. In this case the three most common designs are the 'path' the 'star' and the 'complete' graph structure. However, Arquilla and Ronfeldt (2001) argue that hybrid forms are also good candidates.

Explicit topologies of covert networks, based on theoretical considerations, are usually not provided. Therefore, it is important to develop a more general framework in which the structure of a covert network can be predicted and analyzed. Terrorist organizations, and more in general covert organizations, constantly face the dilemma between secrecy and operational capability. Baker and Faulkner (1993) discuss the structure of covert organizations and conclude that the requirement for secrecy distinguishes the covert organization from the overt organization: "every secret organization has to solve a fundamental dilemma: how to stay secret and at the same time ensure the necessary coordination and control of its members". In this paper we analyze the question which network structure design should be adopted taking the above mentioned dilemma explicitly into account. That is, we consider both secrecy and information processing efficiency as key network design parameters and we analyze several different scenarios corresponding to different assumptions on those parameters. The first scenario corresponds to the situation of a covert operation in its initial phase in a hostile environment. We assume that it is equally likely for network members to be exposed and upon exposure of an individual all communication of this individual with others is detected. In the second scenario we assume that an initial operation is conducted in an environment of varying hostility. That is, we assume that there is a certain fixed probability that communication of any exposed individual with others is intercepted. Finally, we consider the scenario of a covert operation in a hostile environment that passed its initial stage. That is, we assume that exposure of an individual depends on his centrality with regard to information exchange and upon exposure all his communication with others is detected.

The relationships between individuals in a covert organization are modeled as a graph. A vertex can be interpreted as either an individual, a terrorist cell or a military unit. In the latter two cases we view a cell (or unit) as a single operational entity and we are interested in the communication structure among cells (units). There exists an edge between two individuals whenever there is an exchange of information between the corresponding vertices on a regular basis. The exchange of information for instance may represent the fact that one individual facilitates weapons or false documents to another, or it may represent target selection information exchange between differing cells. The underlying idea is that for the covert organization to execute a mission successfully cooperation and coordination are necessary.

Secrecy will be defined by using two parameters: the exposure probability and the link detection probability. In different scenarios these parameters will be varied. The information measure is modeled in two ways, mainly to check the robustness of our results. First the average distance is used in defining the network performance in the sense of information. Second a worse-case performance bound of information exchange is taken by modeling the information measure using the diameter of the underlying graph. Under the assumption of uniform exposure probability of network members (an operation in its initial stage) we will show that either the all-to-all graph or star graph is the optimal design solution, depending on the link detection probability. We show that cellular networks are optimal if the exposure probability of network members depends on the network structure.

In section 2 graph theoretical preliminaries will be discussed. The tradeoff between information and secrecy, and the corresponding Nash bargaining problem, will be discussed in section 3. In section 4 (approximate) optimal covert networks will be established for several different scenarios regarding secrecy. To indicate the robustness of the results a variation on the information measure and its corresponding optimal networks will be discussed in section 5. Section 6 concludes the paper.

2 Graph Theoretical Preliminaries

In this section we present preliminaries from graph theory. For a general overview we refer to Bollobas (1998). Note that the word *graph* and *network* will be used interchangeably throughout the text.

A graph g is an ordered pair (V, E), where V represents the finite set of vertices and the set of edges E is a subset of the set of all unordered pairs of vertices. An edge $\{i, j\}$ connects the vertices i and j and is also denoted by ij. The order of a graph is the number of vertices $|V|$ and the size equals its number of edges $|E|$. The set of all graphs of order n and size m is denoted with $\mathbb{G}(n, m)$. The set of graphs of order n is denoted by $\mathbb{G}^n$. In this paper we are only interested in connected graphs because we study the organizational form of groups in which the actions of individuals are coordinated. Therefore each graph under consideration is assumed to be connected. The degree of a vertex is the number of vertices to which it is connected. We denote the degree of vertex i in graph g by $d_i(g)$. The star graph on n vertices is denoted by g^n_{star}. We denote a ring graph of order n with g^n_{ring} and a path graph of order n with g^n_{path}. A complete graph of order n is denoted with g^n_{comp}. See Figure 1 for an illustration of these graphs of order 5. The shortest distance (in number of edges one has to travel) between vertex i and j is called the geodesic distance between i and j. The geodesic distance between vertices i, j in g is denoted by $l_{ij}(g)$. Clearly, $l_{ij}(g) = l_{ji}(g)$. We will write l_{ij} instead of $l_{ij}(g)$ if there can be no confusion about the graph under consideration. The total distance $T(g)$ in the graph $g = (V, E)$ is defined by $\sum_{i,j} l_{ij}(g) = \sum_{i \in V} \sum_{j \in V} l_{ij}(g)$. The diameter $D(g)$ of a graph $g = (V, E)$ is defined to be the maximum over the geodesic distances between all pairs of vertices, i.e. $D(g) = \max_{(i,j) \in V \times V} l_{ij}(g)$. Furthermore, we assume without loss of generality that $n \geq 3$.

Example 1: In figure 1 a star graph, a ring graph, a path graph and a complete graph, all of order 5, are provided.

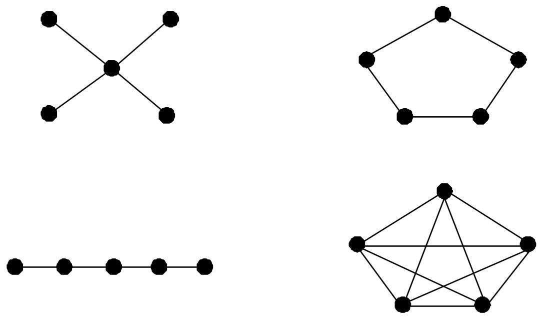

Figure 1: Star graph of order 5 (top left), ring graph of order 5 (top right), path graph of order 5 (down left) and complete graph of order 5 (down right).

	$T(g)$	$D(g)$
g^5_{star}	32	2
g^5_{ring}	30	2
g^5_{path}	40	4
g^5_{comp}	20	1

Table 1: Total distance and diameter for several order 5 graphs

We list the total distance and diameter of each graph in Table 1. For instance, the star graph g^5_{star} has one vertex with distance 1 to all the other vertices (the center vertex) and all other vertices have distance 1 to the center vertex and distance 2 to the remaining three vertices. Therefore $T(g^5_{star}) = 4 + 4(1 + 2 \cdot 3) = 32$. Clearly, the maximum of the geodesic distances in the star graph equals 2: $D(g^5_{star}) = 2$.
For the four standard types of graphs the total distances are provided in Lemma 2.1, the proof of which can be found in the appendix.

Lemma 2.1

(i) $T(g^n_{star}) = 2(n-1)^2$

(ii) $T(g^n_{ring}) = \begin{cases} \frac{n^3-n}{4} & \textit{if } n \textit{ is odd} \\ \frac{n^3}{4} & \textit{if } n \textit{ is even} \end{cases}$

(iii) $T(g^n_{path}) = \frac{(n-1)n(n+1)}{3}$

(iv) $T(g^n_{comp}) = n(n-1)$

3 The Tradeoff between Information and Secrecy

Usually in graphs the time delay for sending information from one vertex to the other is assumed to be proportional to the number of edges the information must travel. In covert networks the higher the number of edges a 'message' must travel the more likely it becomes that it will be intercepted. The average performance, $I(g)$, of a network $g \in \mathbb{G}^n$ in the sense of information is therefore defined by the (normalized) reciprocal of the total distance,

$$I(g) = \frac{n(n-1)}{T(g)}.$$

Since $T(g) \geq n(n-1)$ for any $g \in \mathbb{G}^n$ it follows that $0 \leq I(g) \leq 1$. If $I(g) > I(g')$, then in network g it is easier (in an average sense) to send information around than in network g'. If everybody is able to communicate with everybody else, information can flow freely which gives the best information performance: $I(g^n_{comp}) = 1$.

Example 2: Consider the complete graph g^5_{comp}, the star graph g^5_{star}, the path graph g^5_{path} and the ring graph g^5_{ring} as in Example 1. It follows that $I(g^5_{comp}) = 1$, $I(g^5_{star}) = \frac{5}{8}$, $I(g^5_{path}) = \frac{1}{2}$ and $I(g_{ring}) = \frac{2}{3}$. Thus we have, $I(g^5_{comp}) > I(g^5_{ring}) > I(g^5_{star}) > I(g^5_{path})$.

The performance of the network $g = (V, E)$ in sense of secrecy will be indicated by $S(g)$. We assume that there are two factors for each individual in the network that contribute to this secrecy. Consider for instance the case of Nawaf al Hazmi, selected by Bin Laden as one of the suicide operatives for the 9-11 operation. As discussed in the 9-11 Commission Report: "U.S. intelligence would analyze communications associated with Midhar whom they identified during this travel, and Hazmi, whom they could have identified but did not." (Kean et al. 2002). Thus first, there is a certain probability $\alpha_i(g)$ that upon surveillance individual i will be exposed as member of the network, and second if i is detected he will expose a fraction of the network which is represented by $1 - u_i(g)$.

We define the secrecy measure $S(g)$ by

$$S(g) = \sum_{i \in V} \alpha_i(g) u_i(g)$$

where u_i reflects the fraction of the network that remains unexposed when i is detected. This measure thus reflects the expected fraction of the network that remains undetected. Furthermore we define,

$$\mu(g) = S(g)I(g) \tag{1}$$

as a total performance measure or criterion to compare graphs. A motivation for this choice is provided below.

Imagine that there are two agents responsible for setting up a covert operation, one tasked with minimizing the danger of exposure and the other one tasked with ensuring sufficient communication possibilities between members. The agents bargain over the set of all possible connected networks. The bargaining will eventually result in a network structure. This approach differs from traditional network formation models where equilibrium requirements are analyzed such that individuals do not benefit from altering the structure of the network. In those models network formation is considered to be a local process (see for instance Jackson 2001). Individuals form or break links according to some local criterion. Instead, we consider the formation of a network in such a way that all individuals are willing to adopt a global network structure that is optimal (in a bargaining sense) in the possibility to coordinate while maintaining secrecy.

We thus model the problem of finding an optimal graph of given order by analyzing the tradeoff between secrecy and operational efficiency as a two-person finite Nash bargaining problem. A two-person finite bargaining problem is a pair $(F, 0)$ where $F \subset \mathbb{R}^2$ is a finite set of feasible outcomes and $0 \in F$ represents the disagreement point. Let $\mathbb{B}$ denote the class of all finite bargaining problems of this type. In our setting the set of feasible outcomes equals $F_* \equiv \{(S(g), I(g)) | g \in \mathbb{G}^n\}$, where each point $(S, I) \in F_*$ corresponds to those graphs $g \in \mathbb{G}^n$ with secrecy measure $S(g) = S$ and information measure $I(g) = I$.
A bargaining solution ϕ assigns to each $(F, 0) \in \mathbb{B}$ a non empty subset $\phi((F, 0))$ of F. The Nash bargaining solution, $N(F, 0)$, is defined by

$$N(F, 0) = argmax \quad \{x_1 x_2 | x = (x_1, x_2) \in F\} \quad \text{for all } (F, 0) \in \mathbb{B}.$$

In our application the Nash bargaining solution will lead to those graphs that maximize the product of secrecy and information measure, that is

$$N(F_*, 0) = argmax \quad \{\mu(g) = S(g)I(g) | g \in \mathbb{G}^n\}.$$

The Nash bargaining solution can be motivated on the basis of the following general properties which have a strong appeal in our application framework.

1. For all $x = (x_1, x_2) \in \phi((F, 0))$: if $t = (t_1, t_2)$ such that $t_1 > x_1$ and $t_2 > x_2$, then $t \notin F$
2. Let F be such that for all $(x_1, x_2) \in F$ it also holds that $(x_2, x_1) \in F$. Then $(x_1, x_2) \in \phi((F, 0))$ implies $(x_2, x_1) \in \phi((F, 0))$.
3. If $F \subset G$ and $\phi(G) \cap F \neq \emptyset$, then $\phi(F) = \phi(G) \cap F$.
4. Let $\tau : \mathbb{R}^2 \mapsto \mathbb{R}^2$ be a positive linear transformation given by $\tau(x) = (\lambda_1 x_1, \lambda_2 x_2)$, with $\lambda_1, \lambda_2 > 0$, for all $x = (x_1, x_2) \in \mathbb{R}^2$. Then $\phi(\tau(F)) = \tau(\phi(F))$.

The first property, called *Weak Pareto Optimality* (WPO), translated to our framework, states that for any 'optimal graph' there can not be another graph which has both a higher secrecy measure and information measure. The second property of *Symmetry* (SYM) simply states that the secrecy measure and information measure are equally relevant. The third property, *Independence of Irrelevant Alternatives* (IIA), states that if the set of networks about which the agents bargain is reduced, those solutions of the larger bargaining problem that are still available should form the solutions of the smaller bargaining problem. The final property, *covariance with positive scale transformations* (COV), states that a positive scaling of the secrecy and information measure (i.e., changing units of measurement) rescales the bargaining outcome in the corresponding way. In fact, the Nash bargaining solution is characterized by the above four properties:

Theorem 3.1 *(Mariotti 1998) Let ϕ be a bargaining solution on $\mathbb{B}$. Then $\phi = N(F, 0)$ if and only if ϕ satisfies WPO, SYM, IIA and COV.*

4 Optimal Structures of Covert Networks

In this section we analyze several different scenarios and present network design solutions for each. In section 4.1 it is assumed that individuals in the network are exposed randomly and that upon exposure of an individual all his links with other members are detected. The main result under those assumptions is that the network's optimal structure is that of a star graph.

In section 4.2 it is assumed that with probability p communication over a link will be detected independently and identically for all links. It will be shown that the optimal network structure will be that of the complete graph for low values of p, and the star graph for high values of p, extending the result of section 4.1. Finally, in section 4.3 it is shown that if the network structure is taken into account in defining the exposure probability of individuals and that if upon exposure all links of this individual are detected the resulting optimal network structures are cellular. Exact results are given for $n \leq 7$ and algorithms are developed to analyze higher order graphs.

4.1 Scenario 1: Detecting all links of an exposed individual

Initially we define the secrecy individual i 'contributes' to the network as the fraction of individuals that remain unexposed when upon monitoring individual i all his links with his neighbors are detected. That is, for $g \in \mathbb{G}^n$

$$u_i(g) = 1 - \frac{d_i(g)+1}{n}.$$

Moreover we set $\alpha_i = \frac{1}{n}$. That is, we assume that individuals are uniformly exposed as being a member of the network.
Let $g \in \mathbb{G}(n,m)$. It follows that (using subscript 1 to explicitly denote the scenario),

$$S_1(g) = \frac{1}{n}\sum_{i \in V} u_i(g) = \frac{n^2-n-2m}{n^2}.$$

With $I(g) = \frac{n(n-1)}{T(g)}$ reflecting the average (information) measure of g and

$$\mu_1(g) = S_1(g)I(g),$$

we derive that,

$$\mu_1(g) = \frac{n^2-n}{n^2} \cdot \frac{n^2-n-2m}{T(g)}. \tag{2}$$

Example 3: Reconsider the graphs of Example 1. The values for the secrecy measure, information measure and total performance measure of order 5 graphs corresponding to the first scenario are given in Table 2 below.

	$S_1(g)$	$I_1(g)$	$\mu_1(g)$
g^5_{star}	$\frac{12}{25}$	$\frac{5}{8}$	$\frac{3}{10}$
g^5_{ring}	$\frac{10}{25}$	$\frac{2}{3}$	$\frac{4}{15}$
g^5_{path}	$\frac{12}{25}$	$\frac{1}{2}$	$\frac{6}{25}$
g^5_{comp}	0	1	0

Table 2: Secrecy, information and bargaining criterion of order 5 graphs, scenario 1.

We will show that no graph of order n performs better than g^n_{star}. To do this we first derive a lower bound for the total distance $T(g)$.

Lemma 4.1 *Let $g \in \mathbb{G}(n,m)$. Then $T(g) \geq 2n(n-1) - 2m$*

Proof: Since g has size m, there are exactly m tuples $\{i,j\}$ of vertices for which $l_{ij} = 1$. For all other $\frac{n(n-1)}{2} - m$ tuples $\{i,j\}$ it holds that $l_{ij} \geq 2$. Hence $T(g) \geq (m + 2(\frac{n(n-1)}{2} - m)) \cdot 2 = 2n(n-1) - 2m$.
□

Theorem 4.1 *$\mu_1(g^n_{star}) \geq \mu_1(g)$ for all $g \in \mathbb{G}^n$*

Proof: Suppose there exists a $g \in \mathbb{G}(n,m)$ such that $\mu_1(g) > \mu_1(g^n_{star})$.
Then $\frac{n^2-n-2m}{T(g)} > \frac{n-2}{2(n-1)}$ or equivalently, $T(g) < (2n(n-1)-4m)\frac{n-1}{n-2}$.
However, one readily checks that $(2n(n-1)-4m)\frac{n-1}{n-2} \leq 2n(n-1)-2m$.
Hence, $T(g) < 2n(n-1)-2m$, contradicting Lemma 4.1.□

4.2 Scenario 2: Detecting links with probability p

In this paragraph we assume that whenever an individual in the network is being monitored communication between him and one of his neighbors is detected independently with probability p. The case where $p = 1$ therefore corresponds to the first scenario as analyzed in the previous section. If individual i has d_i neighbors the number of neighbors that will be detected is binomially distributed. Consequently we define,

$$u_i(g) = 1 - \frac{pd_i + 1}{n}$$

and again assume $\alpha_i = \frac{1}{n}$. Therefore we have, for $g \in \mathbb{G}(n,m)$

$$S_2(g) = \frac{n^2 - n - 2pm}{n^2}.$$

With $I(g)$ as before we find

$$\mu_2(g) = S_2(g)I(g) = \frac{n^2-n}{n^2} \cdot \frac{n^2-n-2pm}{T(g)}. \tag{3}$$

For low values of p the complete graph maximizes μ_2.

Theorem 4.2 *If $p \in [0, \frac{1}{2}]$, then $\mu_2(g^n_{comp}) \geq \mu_2(g)$ for all $g \in \mathbb{G}^n$.*

Proof: Note that $T(g_{comp}) = n(n-1)$ and hence $\mu_2(g^n_{comp}) = \frac{n^2-n}{n^2} \cdot (1-p)$. Suppose there exists a $g \in \mathbb{G}(n,m)$ such that $\mu_2(g) > \mu_2(g^n_{comp})$ then $\frac{n^2-n-2pm}{T(g)} > (1-p)$, or equivalently $T(g) < \frac{n^2-n-2pm}{1-p}$. However, one readily checks that for all $p \in [0, \frac{1}{2}]$ $\frac{n^2-n-2pm}{1-p} \leq 2n(n-1)-2m$. Hence $T(g) < 2n(n-1)-2m$, contradicting Lemma 4.1.□

For high values of p we extend the result of the previous section ($p = 1$).

Theorem 4.3 *If $p \in [\frac{1}{2}, 1]$, then $\mu_2(g^n_{star}) \geq \mu_2(g)$ for all $g \in \mathbb{G}^n$*

Proof: Note that $T(g^n_{star}) = 2(n-1)^2$ and $\mu_2(g^n_{star}) = \frac{n^2-n}{n^2} \cdot \frac{n-2p}{2(n-1)}$. Suppose there exists a $g \in \mathbb{G}(n,m)$ such that $\mu_2(g) > \mu_2(g^n_{star})$. Then $\frac{n^2-n-2pm}{T(g)} > \frac{n-2p}{2(n-1)}$ or equivalently
$T(g) < \frac{2(n-1)(n^2-n-2pm)}{n-2p}$. For $p \in [\frac{1}{2}, 1]$ however, it is readily verified that
$\frac{2(n-1)(n^2-n-2pm)}{n-2p} \leq 2n(n-1)-2m$, contradicting Lemma 4.1.□

In case $p = \frac{1}{2}$ it follows from Theorem 4.2 and Theorem 4.3 that μ_2 is maximal for both g_{star} and g_{comp}. However, for $p = \frac{1}{2}$ it is not the case that all graphs maximize μ_2: $\mu_2(g^5_{comp}) = \mu_2(g^5_{star}) = \frac{10}{25}$ whereas $\mu_2(g^5_{ring}) = \frac{8}{25}$.

4.3 Scenario 3: Non-uniform exposure probability

Up to now we assumed that $\alpha_i = \frac{1}{n}$ for all $i \in V$. It can be argued that this is the case when a covert operation is in its initial phase. However, if an operation passed its initial stage the probability of exposure will vary among network members. This because certain individuals, due to a more central position in the network, are more likely to be discovered. We model this 'information centrality' by the equilibrium distribution of a random walk on the graph. This random walk chooses its next vertex at random from the neighbors of the current vertex including itself. For $g \in \mathbb{G}(n, m)$, the equilibrium distribution is denoted by $\pi = (\pi_1, ..., \pi_n)$ and is given by $\pi_i = \frac{d_i+1}{2m+n}$, see for instance Tijms (2003). We set $\alpha_i = \pi_i$ and choose,

$$u_i(g) = 1 - \frac{d_i + 1}{n}$$

It follows that

$$\begin{aligned} S_3(g) &= \sum_{i \in V} \pi_i u_i(g) \\ &= \frac{2m(n-2) + n(n-1) - \sum_{i \in V} d_i^2}{(2m+n)n}. \end{aligned}$$

With

$$I(g) = \frac{n(n-1)}{T(g)}$$

we derive

$$\mu_3(g) = \frac{(n-1)}{2m+n} \cdot \frac{2m(n-2) + n(n-1) - \sum_{i \in V} d_i^2}{T(g)} \tag{4}$$

We obtain explicit expressions of equation μ_3 for the standard graphs. The proof is straightforward (using lemma 2.1), and therefore omitted.

Theorem 4.4

(i) $\mu_3(g^n_{comp}) = 0$

(ii) $\mu_3(g^n_{star}) = \frac{n-2}{3n-2}$

(iii)

$$\mu_3(g^n_{ring}) = \begin{cases} \frac{4(n-1)(n-3)}{n^3} & \text{if } n \text{ is even} \\ \frac{4(n-3)}{n(n+1)} & \text{if } n \text{ is odd} \end{cases}$$

(iv) $\mu_3(g^n_{path}) = \frac{3(n-2)(3n-5)}{n(3n-2)(n+1)}$

Comparing the expressions provided in Theorem 4.4 we obtain

Corollary 4.1

(i) $\mu_3(g^4_{path}) > \mu_3(g^4_{star}) > \mu_3(g^4_{ring}) > \mu_3(g^4_{comp})$

(ii) $\mu_3(g^5_{ring}) > \mu_3(g^5_{path}) = \mu_3(g^5_{star}) > \mu_3(g^5_{comp})$

(iii) $n = \{6, 7, 8\}$*:* $\mu_3(g^n_{ring}) > \mu_3(g^n_{star}) > \mu_3(g^n_{path}) > \mu_3(g^n_{comp})$

(iv) $n = \{9, ...\}$*:* $\mu_3(g^n_{star}) > \mu_3(g^n_{ring}) > \mu_3(g^n_{path}) > \mu_3(g^n_{comp})$

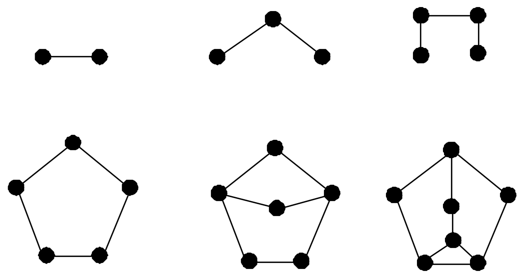

Figure 2: Optimal graphs for scenario 3 for $n \in \{2, ..., 7\}$, with average information measure.

The graphs $g \in \mathbb{G}^n$ that maximize $\mu_3(g)$ for $n = 2, ..., 7$ are shown in figure 2.

It can be seen that the optimal networks adopt a cellular structure. For large values of n it is not possible to calculate exact solutions and we resort to a simulation technique. We provide two algorithms to approximate the graph that maximizes μ_3. The first algorithm (I) randomly generates a graph. Each edge is present with probability $\frac{1}{2}$. If the resulting graph g is connected $\mu_3(g)$ is computed and stored. Next another graph g' is generated and $\mu_3(g')$ is compared to $\mu_3(g)$. If $\mu_3(g') > \mu_3(g)$ the graph g is replaced by g'. If not, g is kept. This process is iterated for 500.000 times.

The second algorithm (II) is local in nature. The starting point is a connected graph g of small size (a tree or a ring graph for instance) for which $\mu_3(g)$ is computed. Next edges are randomly added one by one as long as this increases the value of μ_3. The algorithm ends when adding a single edge does not increase the value of μ_3. Different starting graphs may result in different outcomes. Therefore several starting graphs are tried and the one yielding the graph g' with maximum $\mu_3(g')$ is selected. Finally, the outcomes of algorithm I and II are compared and the graph with the highest value for μ_3 is selected as the approximate solution for our μ_3 maximization problem.

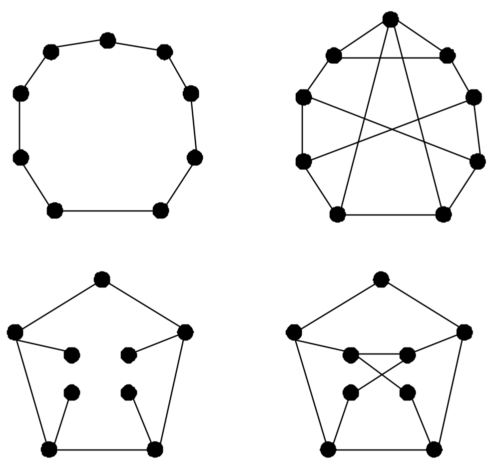

Figure 3: Local optimization starting graphs (top left and down left) and their resulting approximate optimal graphs (top right and down right respectively).

Example 6: Consider $n = 9$. Using algorithm I we generated and compared 500.000 connected graphs yielding the best graph shown in Figure 3 above (down right) with a total performance measure of 0.3348. The second algorithm was run starting from several different small order graphs of which two are shown in the same figure. Local optimization starting from the down left tree resulted in the down right graph, the same as resulted from algorithm I. Starting algorithm II from the top left graph resulted in the graph g shown in the top right, for which $\mu_3(g) = 0.3355$. Actually, using other initial graphs did not yield a graph with a higher value of μ_3.

In Figure 4 we present the results of this process for graphs of order $n = 8, 9$, and 10 respectively.

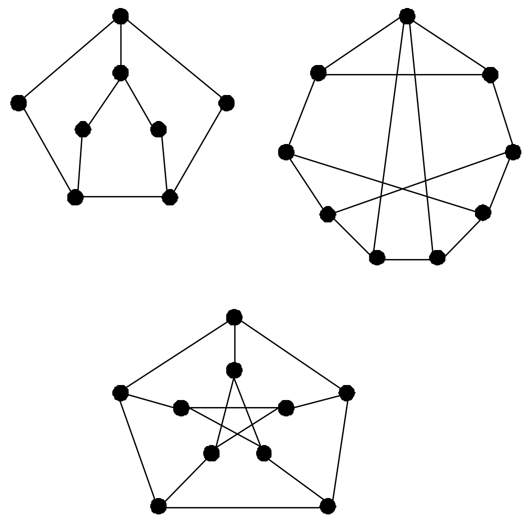

Figure 4: Approximate optimal graphs for scenario 3, for order 8,9 and 10.

It can be seen that for $n = 10$ the Petersen graph appears to approximate the optimal one.

Finally Figure 5 depicts approximate optimal graphs for some larger values of n: $n = 25$ and $n = 40$.

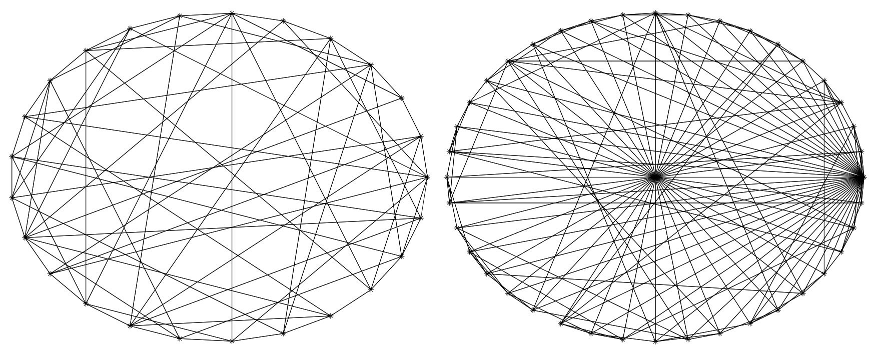

Figure 5: Approximate optimal graphs for scenario 3, for n=25 (left) and n=40 (right), average information measure.

It can be seen that for $n = 25$ a cellular structure emerges. The degree varies between 5 and 7. For the approximate optimal graph of order 40 also cellular structures appear but now it can be seen that a central individual emerges (not connected to everyone but with high degree) around which smaller cells are distributed.

5 A Variation on the Information Measure

The analysis so far has been conducted with information performance measured by the (normalized) reciprocal of the total distance in the network. This information measure represented the *average* performance of the network with respect to the exchange of information. Here we repeat the analysis, using an information measure taking worst case performance into account. Actually, in considering problems in communication over networks or circuit layout optimization often the diameter is considered to be the decisive parameter (Chung 1987). We define the worst case performance information measure $\overline{I}(g)$ by

$$\overline{I}(g) = \frac{1}{D(g)}. \tag{5}$$

We use the upper bar to explicitly differentiate this measure from the information measure used before. Obviously $0 \leq \overline{I}(g) \leq 1$ and $\overline{I}(g_{comp}) = 1$. Moreover, if $\overline{I}(g) > \overline{I}(g')$, then worst case performance in g is better than in g'.

First consider scenario 1: uniform exposure probability and detection of all links. For $g \in \mathbb{G}(n, m)$ with,

$$S_1(g) = \frac{n^2 - n - 2m}{n^2}$$

and $\overline{I}(g)$ as in equation (5) we have,

$$\overline{\mu}_1(g) = S_1(g)\overline{I}(g) = \frac{n^2 - n - 2m}{D(g)n^2}. \tag{6}$$

It turns out that g^n_{star} maximizes $\overline{\mu}_1$ over $\mathbb{G}^n$.

Theorem 5.1 *For all $g \in \mathbb{G}^n$, $\overline{\mu}_1(g^n_{star}) \geq \overline{\mu}_1(g)$*

Proof: Let $g \in \mathbb{G}(n, m)$. Clearly $m \geq n - 1$ (we only consider connected graphs). With $\overline{\mu}_1(g^n_{star}) = \frac{(n-1)(n-2)}{2n^2}$ it follows readily that $\overline{\mu}_1(g) > \overline{\mu}_1(g_{star})$ implies $D(g) < 2$. This however would lead to $D(g) = 1$ and thus $g = g_{comp}$. Since $\overline{\mu}_1(g_{comp}) = 0$ we arrive at a contradiction. □

Next we consider scenario 2 with a probability p of link detection, again assuming uniform exposure of individuals. Using the worst case performance information measure $\overline{I}(g)$ and secrecy measure

$$S_2(g) = \frac{n^2 - n - 2pm}{n^2}$$

we have for all $g \in \mathbb{G}(n, m)$,

$$\overline{\mu}_2(g) = S_2(g)\overline{I}(g) = \frac{n^2 - n - 2pm}{D(g)n^2} \tag{7}$$

Theorem 5.2 *For all $g \in \mathbb{G}^n$ and all $p \in [0, 1]$, we have,*

(i) $\overline{\mu}_2(g^n_{comp}) \geq \overline{\mu}_2(g)$ *if* $p \leq \frac{n}{2(n-1)}$

(ii) $\overline{\mu}_2(g^n_{star}) \geq \overline{\mu}_2(g)$ *if* $p \geq \frac{n}{2(n-1)}$

Proof: If $g \in \mathbb{G}^n$ is such that $\overline{\mu}_2(g) > \overline{\mu}_2(g_{star})$ then $D(g) = 1$ and consequently $g = g^n_{comp}$. Note that $\overline{\mu}_2(g_{comp}) = \frac{(n^2-n)(1-p)}{n^2}$ and $\overline{\mu}_2(g_{star}) = \frac{n^2-n(1+2p)+2p}{n^2}$. Therefore $\overline{\mu}_2(g^n_{comp}) \geq \overline{\mu}_2(g^n_{star})$ if and only if $p \leq \frac{n}{2(n-1)}$. □

Finally we analyze scenario 3 (non-uniform exposure probability). With secrecy measure for $g \in \mathbb{G}(n,m)$ given by

$$S_3(g) = \frac{2m(n-2) + n(n-1) - \sum_{i \in V} d_i^2}{(2m+n)n}$$

it follows that

$$\overline{\mu}_3(g) = S_3(g)\overline{I}(g) = \frac{2m(n-2) + n(n-1) - \sum_{i \in V} d_i^2}{D(g)(2m+n)n} \tag{8}$$

The graphs $g \in \mathbb{G}^n$ that maximize $\overline{\mu}_3$ for $n \in \{2, ..., 7\}$ are provided in Figure 6.

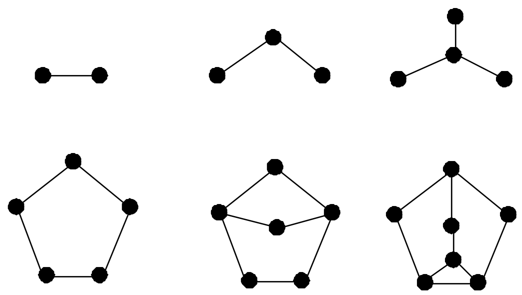

Figure 6: Optimal graphs for scenario 3 with $n \in \{2, ..., 7\}$, worst-case information measure.

It can be seen that the optimal graphs are similar to those for scenario 3 with $I(g) = \frac{n(n-1)}{T(g)}$ (see figure 2). Only the optimal graph of order $n = 4$ is different. This shows the robustness of our results.

Finally we present approximate optimal graphs for larger orders, using the same approximation technique as explained in the section 4.

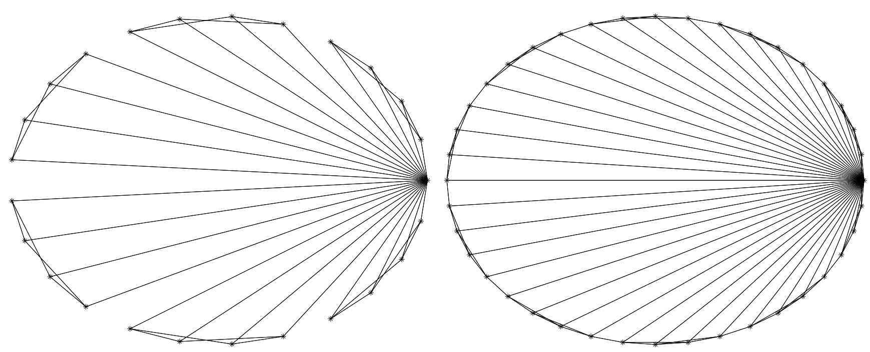

Figure 7: Approximate optimal graphs for scenario 3 with n=25 (left) and n=40 (right), worst-case information measure.

6 Conclusion

In this paper we have analyzed the dilemma every covert organization faces: how to stay secret and at the same time ensure good coordination. We modeled the structure of a covert organization as an undirected graph. The vertices can either be interpreted as individuals in the organization, military units or as terror cells. The selection of the optimal organizational structure was modeled as a bargaining problem between an agent responsible for the secrecy of the organization and another one responsible for ensuring operational efficiency.

Different scenarios were developed and analyzed by assigning a specific information measure and a specific secrecy measure to the set of connected graphs. The first scenario corresponded to a covert organization conducting an operation in its initial stage, in a hostile environment. We established that centralizing information flow by adopting a star network is optimal. The second scenario consisted of a covert organization in its initial stages in an environment of varying hostility. We established that all-to-all communication is optimal in a friendly environment (for instance in a safe-house) and that the star network is optimal in a hostile environment. Finally, the communication structure of a covert network that passed its initial stages in a hostile environment was analyzed (i.e., jihadi networks in Europe). In the event of such a scenario we established that cellular networks are optimal.

Our results are consistent with the apparent organizational forms of current terrorist networks, particularly Al Qaeda's 'network of networks'. The results are of twofold use. First they predict the structure of terrorist networks which is important to be able to detect and combat them. Second they aid in the design of military network structures that have to depend on stealth and secrecy (i.e., military swarming). Finally, the analysis in this paper presents a quantitative theoretical framework for reasoning about covert networks.

A Appendix

Proof of lemma 2.1:

(i) Denote the center vertex of g^n_{star} with index c. Clearly $\sum_{i\in V} l_{ci}(g^n_{star}) = n-1$. For $j \in V$, $j \neq c$ $\sum_{i\in V} l_{ji}(g^n_{star}) = 1 + 2(n-2) = 2n-3$. Therefore $T(g^n_{star}) = \sum_{i\in V}\sum_{j\in V} l_{ij}(g^n_{star}) = n-1+(n-1)(2n-3) = 2(n-1)^2$.

(ii) First consider the case when n is odd. Then for all $i \in V$: $\sum_{j\in V} l_{ij}(g^n_{ring}) = 2(1+2+...+\frac{n-1}{2}) = \frac{(n-1)(n+1)}{4}$. Hence, $T(g^n_{ring}) = \frac{(n-1)n(n+1)}{4}$ for the case that n is odd. In case n is even it follows that for all $i \in V$: $\sum_j l_{ij}(g^n_{ring}) = 2(1+2+...+(\frac{n}{2}-1)) + \frac{n}{2} = \frac{n^2}{4}$. Therefore $T(g^n_{ring}) = \frac{n^3}{4}$ in case n is even.

(iii) There are $n-1$ tuples $\{i,j\}$ such that $l_{ij}(g^n_{path}) = 1$, $n-2$ tuples $\{i,j\}$ such that $l_{ij}(g^n_{path}) = 2$,..., 1 tuple $\{i,j\}$ such that $l_{ij}(g^n_{path}) = n-1$. Each tuple has to be counted twice, therefore

$$\begin{aligned} T(g^n_{path}) &= 2\{(n-1)+2(n-2)+3(n-3)+...+(n-1)(n-(n-1))\} \\ &= 2\{n+2n+3n+...+(n-1)n-(1+2^2+3^2+...+(n-1)^2)\} \\ &= 2\{n\cdot\sum_{k=1}^{n-1} k - \sum_{k=1}^{n-1} k^2\} \\ &= 2\{\frac{n\cdot n(n-1)}{2} - \frac{(n-1)n(2n-2+1)}{6}\} \\ &= \frac{(n-1)n(n+1)}{3} \end{aligned}$$

(iv) For all $i \in V$ it holds that $\sum_{j\in V} l_{ij}(g^n_{comp}) = n-1$. Thus $T(g^n_{comp}) = n(n-1)$. □

References:

[1] Arquilla, J. and Ronfeldt, D.(2001). Networks and Netwars. Rand Monograph MR-1382. Rand Institute.
[2] Baker, W.E. and Faulkner, R.(1993). The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. *American Sociological Review* 58(12): 837-860.
[3] Bergen, P.(2006). The Osama Bin Laden I Know: an Oral History of al Qaeda's Leader. *Free Press: New York.*
[4] Bollobas, B.(1998). Modern Graph Theory. *Springer-Verlag: New York.*
[5] Chung, F.R.K.(1987). Diameters of Graphs: Old problems and New Results. *Congressus Numerantium* 60: 295-317.
[6] Jackson, M.O.(2001). The Stability and Efficiency of Economic and Social Networks. In: Dutta B. and Jackson M.O., editors. Networks and Groups. *Springer-Verlag: Heidelberg.* p 99-140.
[7] Kean, T.H, Hamilton, L.H., Ben-Veniste, R., Kerrey, B., Fielding, F.F., Lehman, J.F., Gorelick, J.S., Roemer, T.J., Gorton, S. and Thompson, J.R. (2002). The 9-11 Commission Report, Final Report of The National commission on Terrorist Attacks upon the United States. *W.W. Norton & Company, Inc.: New York.*
[8] Mariotti, M.(1998). Nash bargaining Theory when the Number of Alternatives can be Finite. *Social Choice and Welfare* 15(3): 413-421.
[9] Mishal, S. and Rosenthal, M.(2005). Al Qaeda as a Dune Organization: Toward a Typology of Islamic Terrorist Organizations. *Studies in Conflict & Terrorism* 28(4): 275-293.
[10] Nash, J.F.(1950). The Bargaining Problem. *Econometrica* 18(2): 155-162.
[11] Tijms, H.C.(2003). A first course in Stochastic Models. *John Wiley & Sons Ltd: Chichester.*
[12] Tsvetovat, M. and Carley, K.(2005). Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence. *Journal of Social Structure* [Internet]. [Cited 2007 Nov 1]; 6(3). Available from:
http://www.cmu.edu/joss/content/articles/volume6/TsvetovatCarley/index.html
[13] Tucker, D.(2001). What is New about the New Terrorism and How Dangerous is It? *Terrorism and Political Violence* 13(3): 1-14.
[14] Vermaat, E.(2002). Bin Laden's Teror Networks in Europe, Occasional Paper. *The Mackenzie Institute: Toronto.*
[15] Vidino, L.(2007). Current Trends in Jihadi Networks in Europe. *Terrorism Monitor* 5(20): 8-11.