CentER

Discussion Paper

No. 2008–46

ON HETEROGENEOUS COVERT NETWORKS

By Roy Lindelauf, Peter Borm, Herbert Hamers

April 2008

ISSN 0924-7815

TILBURG UNIVERSITY

On Heterogeneous Covert Networks

ROY LINDELAUF [a,b,c] PETER BORM [b] HERBERT HAMERS [b]

April 17, 2008

Abstract

Covert organizations are constantly faced with a tradeoff between secrecy and operational efficiency. Lindelauf, Borm and Hamers (2008) developed a theoretical framework to determine optimal homogeneous networks taking the above mentioned considerations explicitly into account. In this paper this framework is put to the test by applying it to the 2002 Jemaah Islamiyah Bali bombing. It is found that most aspects of this covert network can be explained by the theoretical framework. Some interactions however provide a higher risk to the network than others. The theoretical framework on covert networks is extended to accommodate for such heterogeneous interactions. Given a network structure the optimal location of one risky interaction is established. It is shown that the pair of individuals in the organization that should conduct the interaction that presents the highest risk to the organization, is the pair that is the least connected to the remainder of the network. Furthermore, optimal networks given a single risky interaction are approximated and compared. When choosing among a path, star and ring graph it is found that for low order graphs the path graph is best. When increasing the order of graphs under consideration a transition occurs such that the star graph becomes best. It is found that the higher the risk a single interaction presents to the covert network the later this transition from path to star graph occurs.

Keywords: covert networks, terrorist networks, heterogeneity, game theory, information, secrecy.

JEL classification: C50, C78.

1 Introduction

Recently an increasing interest in the application of methods from social network analysis to the study of terrorism can be observed. For instance in counterinsurgency social network analysis is recognized to be one of the most important tools to describe effects of the operational environment and to evaluate the threat (Petreaus 2007). Moreover, it is realized that methods from several mathematical disciplines are valuable in analyzing covert networks. Sageman (2004) discusses the use of applying the network paradigm (clustering, small-world phenomena, etc.) to analyze terror networks. Social network analysis of specific terror events are available, although not abundant, see for instance Koschade (2005, 2006). There is something to be gained by applying and extending ideas from graph theory and game theory in the analysis of covert networks. Social and affiliation network analysis as well as spatiotemporal point pattern analysis are valuable mathematical methods that certainly warrant further exploration in the analysis of subversive activities, terrorism and guerrilla warfare.

[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

Terrorism is not a topic that is easily researchable on the basis of practical data because of the clandestine nature of terrorist groups (Johnson 2007). Therefore theoretical frameworks that describe how rational actors should behave in trying to attain certain strategic goals can provide insights into the functioning of terrorist groups. For instance, the strategic interaction between economic actors, within an explicitly given network structure, is modeled in Jackson (2001). In this paper we present and extend theoretical insights into the dilemma of secrecy and operational control in covert networks. In Lindelauf et al. (2008) a theoretical framework on the homogeneous communication structure of covert networks is established. A secrecy measure and information measure are defined and the Nash bargaining criterion is adopted to determine optimal covert networks of given order. Several scenarios are analyzed. First, under the assumption of uniform individual exposure probability and high link detection probability it is shown that a star graph is optimal. However, on the assumption of low link detection probability it is shown that the complete graph is optimal. Second, if the exposure probability of individuals depends on their centrality with regard to information exchange it is shown that cellular networks are optimal.

This paper puts the theoretical framework on homogeneous covert networks to the test by applying it to the 2002 Jemaah Islamiyah Bali bombing. The theoretical framework does well in explaining most aspects of the network structure that Jemaah Islamiya adopted to carry out this attack. In addition however it is recognized that the nature of interaction between entities in a covert organization is not necessarily homogeneous. Hence the theoretical framework is extended to incorporate heterogeneity of the network. The most basic heterogeneous network is that in which all but one interaction present similar risks to the organization. The optimal pair of individuals that should conduct the interaction that presents the highest risk to the organization turns out to be the pair that is the least connected to the remainder of the network. In addition, when choosing among a path, star and ring graph with a single high risk interaction pair it is found that for low order graphs the path graph is best. Increasing the order a transition occurs such that the star graph becomes best. It is found that the higher the risk a single interaction presents to the covert network the later this transition from path to star graph occurs. Furthermore, approximate optimal networks given a single risky interaction are determined by simulation.

This paper is organized as follows. After presenting some graph theoretical preliminaries in section 2 secrecy and communication in networks and the main theoretical findings of Lindelauf et al. (2008) will be reviewed in section 3. The Jemaah Islamiyah 2002 Bali bombing operation will be discussed in section 4 and compared to the theoretical results on optimal covert networks. In section 5 the theoretical framework is extended to incorporate the heterogeneity of interaction between entities in covert networks.

2 Preliminaries

In this section we present graph theoretical preliminaries. A good general overview is given by Bollobas (1998).

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 $d_i(g)$. A graph is called k-regular if all vertices have degree k. A star graph on n vertices is denoted by g^n_{star}. We denote a ring graph of order n by g^n_{ring} and a path graph of order n by g^n_{path}. The complete graph of order n is denoted by 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 $n \geq 3$. We denote the set of 'neighbors at distance k' of vertex i by $\Gamma_{i,k}(g)$, i.e., $\Gamma_{i,k}(g) = \{j \in V | l_{ij}(g) = k\}$.

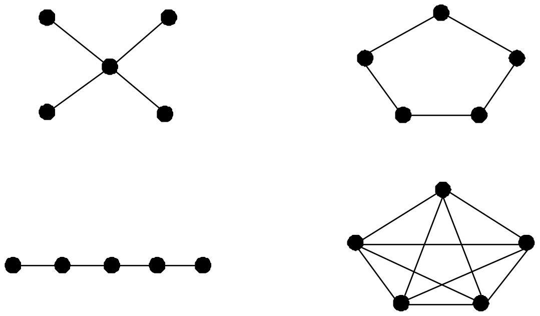


Figure 1: Star graph of order 5 (top left), ring graph of order 5 (top right), path graph of order 5 (down left) and complete graph of order 5 (down right).

3 Secrecy and Communication in Homogeneous Covert Networks

Covert networks are constantly challenged with the tradeoff between secrecy on one side and operational capability on the other side. For instance, consider the failed Israeli covert operation in Egypt known as Operation Susannah (Johnson 2007). Israel's Military Intelligence decided to set up a network of sleeper agents in Egypt which was activated in 1954 to prevent the British withdrawal from Egypt. However, after the arrest of a suspect names of accomplices of the operation were found in his apartment and the network was subsequently dismantled. This example shows that every member of a covert network presents a risk to the secrecy of the network in the sense that upon his exposure potentially others are exposed.

Another example of a covert network that was exposed is the following. During the 1950's a group of lawyers and legal experts that turned against the communist regime in East Berlin were selected by the CIA to be converted to an underground armed resistance group consisting of cells of 3 individuals each (Weiner 2007). However, the network topology of this organization equalled that of a complete graph (the worst possible in the sense of secrecy) because all individuals were acquainted with each other. Upon the exposure of one network member the Soviets discovered and arrested all other members. The operation was a failure.

Another more recent example is that of Al Qaeda. It is currently widely known that Al Qaeda morphed from a bureaucratic, hierarchical organization into an ideological umbrella for loosely coupled jihadi networks (Mishal et al. 2005). We argue that the changing environment pressured the Al Qaeda leadership into adopting network topologies that maintain secrecy while simultaneously providing some possibility to coordinate and control. Videotapes of lecture series from the summer of 2000 show Abu Musab al Suri (Mustafa Setmariam Nasar) explicitly discussing (and providing critique of) hierarchical network structures (Bergen 2006, Cruickshank 2007). Ideally the network should consist of small autonomous cells with limited strategic guidance. However, it is known that in reality there still exist weak bonds between local groups and experienced jihadists or Al Qaeda operatives, such was the case for instance in the Madrid and London attacks (Vidino 2006). What is important is the fact that current covert organizations definitely take the secrecy versus operational efficiency dilemma explicitly into account.

The examples above show that it is important for a covert organization to take the network structure explicitly into account. Operation Susannah and CIA's East Berlin operation illustrated that failing to do this may result in failure of the operation. It appears that current terrorist organizations take their network structure explicitly into account as the example of Al Qaeda shows. In absence of further information we are interested in what structure these organizations actually adopt. In Lindelauf et al. (2008) a theoretical framework for the analysis of the communication structure of covert networks was given. The optimal network structure was derived considering one of several scenarios. Below we recapitulate the theoretical framework and present the main results.

Imagine two agents, one responsible for network secrecy and the other one for information efficiency, bargaining over the set $\mathbb{G}^n$ of connected graphs of given order n. The information measure $I(g)$ of $g \in \mathbb{G}^n$ is given by

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

The secrecy measure $S(g)$ of a graph $g \in \mathbb{G}^n$ is defined as the *expected* fraction of the network that remains unexposed under the assumption of exposure probability of individual $i \in V$ being equal to α_i. The fraction of the network that individual i exposes (including himself) is defined to be $1 - u_i$. Then,

$$S(g) = \sum_{i \in V} \alpha_i u_i. \tag{2}$$

The tradeoff between secrecy and information is modeled as a game theoretic bargaining problem. Hence, the optimal graph in the sense of the Nash bargaining solution is the graph $g \in \mathbb{G}^n$ that maximizes

$$\mu(g) = S(g)I(g). \tag{3}$$

Two scenarios are considered in

Lindelauf et al.(2008). In the first scenario it is assumed that the probability of exposure of an individual in the organization is uniform over all network members, i.e., $\alpha_i = \frac{1}{n}$. Additionally it is assumed that the fraction of the network that individual i exposes is equal to the expected number of neighbors that will be detected if communication on links is detected independently and identically with probability p, i.e., we set $1 - u_i = \frac{pd_i+1}{n}$. The main result is that for a low value of p the complete graph is optimal and for a high value of p the star graph is optimal:

Theorem 3.1

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

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

As an illustration consider the network structure of the former Dutch National Clandestine Service's so-called 'stay behind organization'. After the Second World War it was decided that precautionary measures should be taken such that in the event of a sudden invasion of the Netherlands a covert organization would be present to assist in subversive and covert activities to support the overthrow of the occupying forces (Engelen 2005). This covert organization was divided into two groups: group A and B. Support group 'A' consisted of single agents all equipped with radio systems to connect to the Allied Clandestine Base (ACB). These single agents were not aware of each other because the chosen network structure equalled that of a star graph. Due to the extreme covert nature of this network (which was finally disbanded after the end of the Cold War in 1992) the initial exposure probability of network members may be assumed to be uniform. Communicating with the ACB presented a high link detection probability (high value for p) hence it can be argued that the star network design was an optimal choice. However, after operating for an extended period of time the exposure probability of the single agents would not be uniform anymore but would start to depend on their 'activity' in exchange of information. This alternative scenario is also analyzed in Lindelauf et al. (2008).

In the second scenario it is assumed that the probability of exposure of an individual in the network $g \in \mathbb{G}(n, m)$ depends on his centrality with regard to the exchanging of information in the network. It is argued that setting $\alpha_i = \frac{d_i+1}{2m+n}$ for all $i \in V$ is an adequate choice. The optimal networks for low order graphs are presented in figure 2.

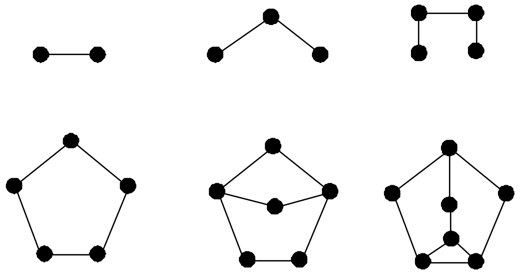


Figure 2: Optimal graphs for $n \in \{2, ..., 7\}$.

Optimal graphs for larger order were approximated by computer simulation and are presented in figure 3. Generally speaking it can be seen that cellular structures emerge: each individual is connected to a limited member of network members.

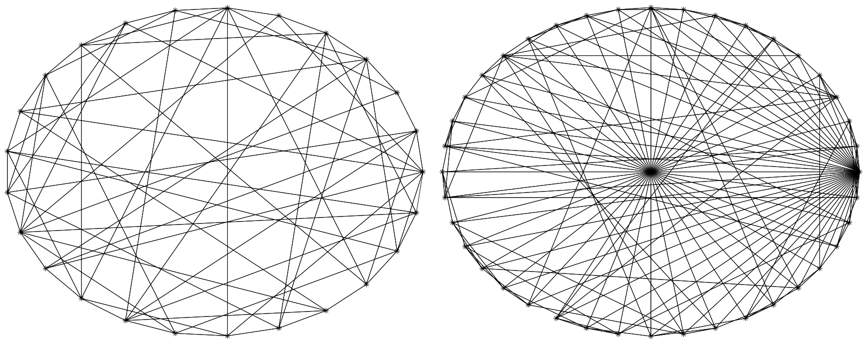


Figure 3: Approximate optimal graphs for n=25 (left) and n=40 (right).

4 Jemaah Islamiya Bali bombing

In this section we analyze an organization that faced the tradeoff between secrecy and operational efficiency. In doing this we put the theoretical framework of Lindelauf et al.(2008) to the test. We analyze how this organization dealt with this tradeoff by studying and comparing the network structure that they adopted to the theoretical framework.

Jemaah Islamiya started as an Indonesian Islamist group and is a loosely structured organization characterized by four territorial divisions (mantiqis) corresponding to peninsular Malaysia and Singapore; Java; Mindanao, Sabah, and Sulawesi; and Australia and Papua (Koschade 2006). Abdullah Sungkar, motivated by the need for a new organisation that could work to achieve an Islamic State in Indonesia, started JI in Malaysia around 1995. Al Qaeda infiltrated JI during the 1990's and JI subsequently developed into a pan-Asian network extending from Malaysia and Japan in the north to Australia in the south (Gunaratna 2002). By doing this Al Qaeda set out to link these groups into a truly transnational network (Abuza 2003).

The tactical operation of the Bali attack that was conducted by Jemaah Islamiyah's Indonesian cell is described in Koschade (2006). The attack was carried out on October 12, 2002, by having a first operative explode a vest of explosives in Paddy's bar. This caused people to flood to the streets, which triggered the second attack by a vehicle based improvised explosive (VBIED) of about 1000 kilograms of TNT and ammonium nitrate. Consequently 202 people were killed. The operational setting consisted of a team of bomb builders located in a safe-house, a separate support team split over two safe-houses and a command team. The individuals in the safe-houses were thoroughly aware of the need for secrecy. This is indicated by the fact that each member used their Balinese alias and that communication occurred in code words. The individuals in the safe-houses rarely left these houses and used methods to reduce the probability of link detection: they only communicated by SMS and they changed their sim cards frequently. Hence, due to the similarity of these individuals from the viewpoint of secrecy the probability of exposure of those individuals may be assumed to be uniform. In terms of the theoretical framework by Lindelauf et al. (2008) described in the earlier section the setting in which these individuals operated reflects the first scenario. Hence, the actual subgraph corresponding to these individuals is best compared to the results obtained for this scenario.

To coordinate the operation a command team consisting of five individuals was set up. The operational commanders were highly active with regard to exchange of information. Hence the setting in which the command team members operated fits best to the second scenario of the theoretical framework. Hence we compare the actual subgraph corresponding to these individuals to the theoretical results obtained for the second scenario in Lindelauf et al. (2008).

Koschade (2006) presents the actual network of this operation as provided in figure 4. It is this graph that we use as basis for comparison with the theoretical framework presented earlier. We partition the network into three subnetworks corresponding to the groups of individuals with intrinsically different goals. The Bali Bombing cell can be split into the bomb making team (cell 18), the support team (team Lima) and the command team. It can be seen that cell 18 as well as team Lima adopted the structure of a complete graph. That is, by choosing a location with tight security, never leaving the house and having someone on guard they tried to lower the exposure probability and link detection probability as much as possible. Both cells obtained the optimal graph according to the theoretical framework. The command team visited both cells and coordinated the operation.

The theoretical framework of Lindelauf et al. only considered a homogeneous communication structure, not the nature of interaction that this communication represents. In his analysis

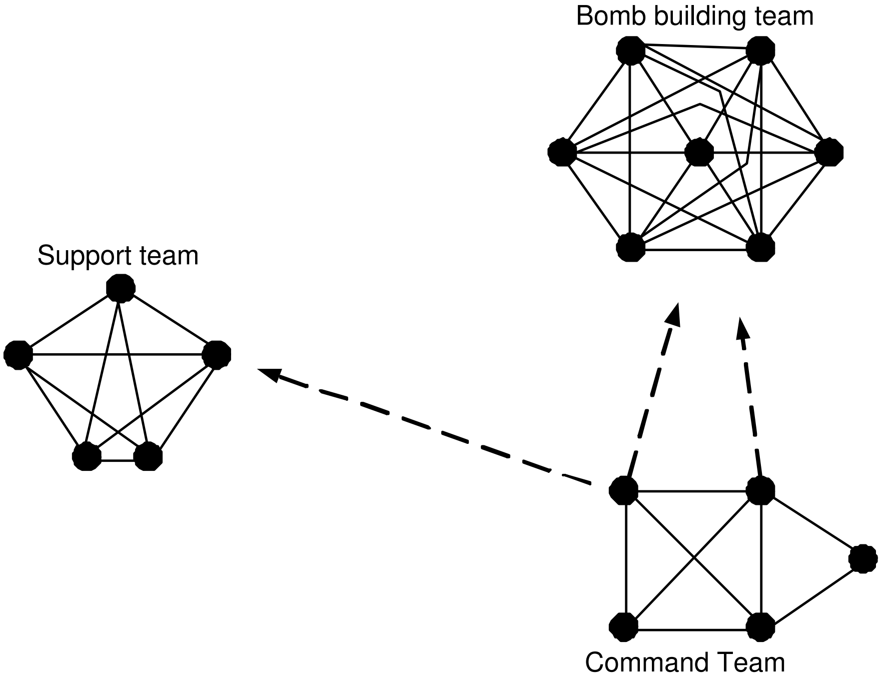


Figure 4: Social Network of Jemaah Islamiyah cell that conducted the Bali Operation on October 6, 2002.

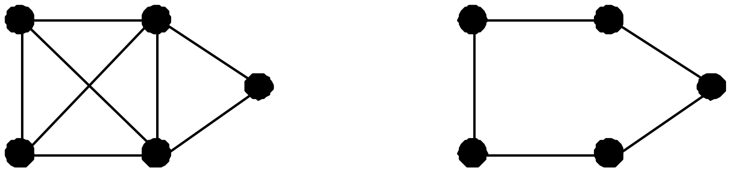


Figure 5: JI Command Team (left) and the theoretically optimal command team (right)

Koschade (2006) considered a weighting function on the edges by scaling the frequency and duration of interaction between 1 and 5. This already indicates that the nature of interaction among individuals in the network is not homogeneous. The frequency and duration of interaction differed most among the members of the subgraph corresponding to the command team. This non-homogeneity of interactions will be incorporated into the theoretical framework in the next section.

5 A First Approach to Heterogeneity in Covert Networks

An organization conducting a covert operation not only has to consider the communication structure of its network but also has to take into account that the nature of interaction between individuals is not homogeneous. For instance, the act of delivering a pre-manufactured bomb to the triggerman is potentially more dangerous than the internal communication (possibly through codewords) discussing the planning of an attack. Therefore in this section we will extend the theoretical framework on covert networks by differentiating between the nature of interaction among network individuals. Two questions come to mind. First, given a network structure which pair of individuals should conduct the interaction that presents the highest risk to the organization? Second, given the fact that there is a pair of individuals conducting an interaction that presents a high risk to the organization which network structure is optimal?

5.1 The Optimal High Risk Interaction Pair

We consider the situation that the interaction between individuals in the network is not completely homogeneous. This among others because the frequency, duration and nature of interaction differs between individuals. Hence, certain interactions present a higher risk to the organization than others. We model this by assigning 'weights' to the links, representing the risk of that interaction. For graph $g = (V, E)$ we define the weighting function $w : E \mapsto [1, \infty)$ such that $w_{ij} > w_{kl}$, $ij, kl \in E$, is interpreted as interaction between individual i and j presenting a higher risk to the organization than interaction between k and l. Denote the set of all such weighting functions by $\mathbb{W}$. Explicitly we denote a graph g with weight $w \in \mathbb{W}$ assigned to its edges by $g(w)$. The interpretation of this weighting function forces us to adjust the definition of secrecy. The information measure needs not to be adapted: one either interacts with an individual or not. However, risky interactions provide an enhanced security threat to the organization.

We adjust the secrecy measure corresponding to the second scenario in Lindelauf et al. (2008). For $g \in \mathbb{G}(n, m)$ we again set $u_i = 1 - \frac{d_i+1}{n}$ but adjust the probability of detection of an individual. This probability of detection not only depends on *the number* of individuals this individual is connected to but also on the nature of that interaction. Let $w_i = \sum_{j \in \Gamma_i(g)} w_{ij}$ where $\Gamma_i(g) = \{j \in V | ij \in E\}$ and define,

$$W = \sum_{i \in V} w_i = 2 \sum_{ij \in E} w_{ij}. \tag{4}$$

Motivated by the fact that a risky interaction increases the relative probability of exposure of an individual we set $\alpha_i = \frac{w_i+1}{W+n}$. In case $w_{ij} = 1$ for all $ij \in E$, α_i reduces to the one in Lindelauf et al.(2008), i.e., $\alpha_i = \frac{d_i+1}{2m+n}$. Secrecy is again defined by

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

It can be seen that the secrecy measure of a graph g is the expected fraction of the network that survives upon exposure of an individual in the network according to probability distribution $(\alpha_i)_{i \in V}$. It is easily derived that

$$S(g) = \frac{n^2 - 2m - n + W(n-1) - \sum_{i \in V} d_i w_i}{n(W+n)}. \tag{5}$$

It follows that $S(g^n_{comp}) = 0$. Slightly more general for any k-regular graph $g \in \mathbb{G}^n$ it holds that $S(g) = 1 - \frac{k+1}{n}$.

With $I(g) = \frac{n(n-1)}{T(g)}$ we find that,

$$\mu(g) = S(g)I(g) = \frac{(n-1)}{T(g)} \frac{n^2 - n - 2m + W(n-1) - \sum_{i \in V} d_i w_i}{W+n}. \tag{6}$$

The following result is readily obtained,

Lemma 5.1

(i) $\mu(g^n_{star}) = \frac{n-2}{2n-2} \cdot \frac{n-1+\frac{1}{2}W}{n+W}$ *if the path is given by 1,2,...,n-1,n.*

(ii) $\mu(g^n_{path}) = \frac{3}{n+1} \cdot \frac{(n-2)(n-1)+(2n-6)W+w_{12}+w_{n-1,n}}{n(W+n)}$.

(iii) $\mu(g^n_{ring}) = \begin{cases} \frac{4n-12}{n(n+1)} & \textit{if } n \textit{ is odd} \\ \frac{4(n-3)(n-1)}{n^3} & \textit{if } n \textit{ is even} \end{cases}$

Due to the symmetry of g_{ring} and g_{star} the interaction that presents the highest risk can be conducted by any pair of individuals. This can also be seen directly from lemma 5.1. In addition we determine the optimal location of the highest risk interaction for the path graph. The best position (in terms of maximizing μ) in the path graph is between either pair of individuals such that one of these individuals is an endpoint of the path. So, if the path is given by $1, 2, ..., n-1, n$ w_{12} or w_{n-1n} is maximal. Thus an organization structured as a path graph does best by having either pair of players conducting the risky interaction as far away as possible from the central players. This is in accordance with intuition.

In general it is shown that the pair of individuals in the organization that should conduct the interaction that presents the highest risk to the organization is the pair that is the least connected to the remainder of the network.

Theorem 5.1 *Let* $g = (V, E) \in \mathbb{G}(n, m)$ *and* $\{kl\} = argmin_{ij\in E}\ (d_i + d_j)$*. Set* $\hat{w}_{kl} = W - (m-1)$*,* $\hat{w}_{ij} = 1$ *for all* $ij \in E \setminus \{kl\}$*. Then* $\mu(g(\hat{w})) > \mu(g(w))$ *for all* $w \in \mathbb{W}$ *with* $\sum_{ij\in E} w_{ij} = W$*.*

Proof: It can be seen from equation 5 that, given a graph $g \in \mathbb{G}(n, m)$ and total weight $W = \sum_{ij\in E} w_{ij}$, maximizing $\mu(g)$ is equal to minimizing $\sum_{i\in V} d_i w_i$. It readily follows that $\sum_{i\in V} d_i w_i = \sum_{ij\in E} w_{ij}(d_i + d_j)$, hence the result follows. □

Given the situation that only a single interaction presents a higher risk to the organization we now compare the optimal path, star and ring graph using these results. We analyze the situation of a slightly riskier interaction ($z = 2$) and the situation of a much more riskier ($z = 100$) interaction. The results are summarized in figure 6. The ring graph is always dominated. It can be seen that for low values of n the path has a higher value of μ than the star graph. At a certain value of n a

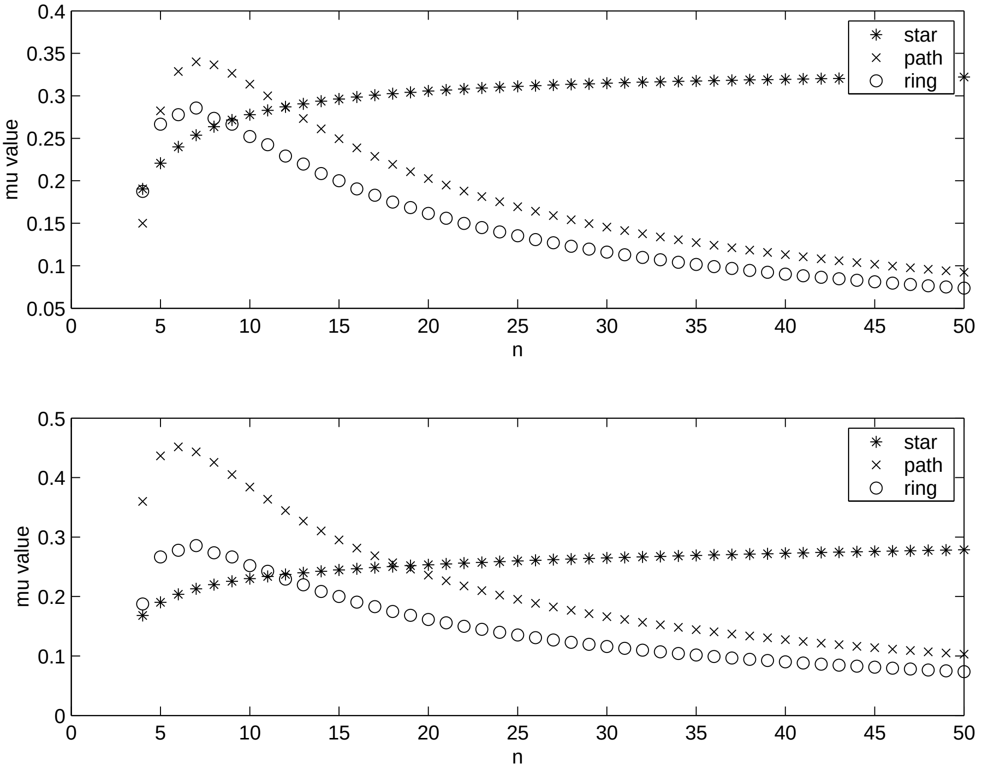


Figure 6: A comparison between star, path and ring graph for z=2 (top) and z=100 (bottom).

transition occurs such that $\mu(g^n_{path})$ becomes smaller than $\mu(g^n_{star})$. In case of $z = 2$ this transition occurs at $n = 11$. In case $z = 100$ this transition occurs at $n = 18$. Thus it can be seen that the amount of risk an interaction poses to the organization influences this transition point. For instance imagine one has to consider an organizational form that either is very centralized (star graph) or decentralized (path graph). If the number of individuals in the organization, n, is very large the star graph is the better choice. This can be understood intuitively because of the difficulty of information exchange in large path graphs as opposed to star graphs. However, if there is a single interaction that is much more risky relative to the others it still is advantageous to adopt a path graph organizational form. Clearly, this reduces the capability to process information but from the perspective of secrecy has the advantage of reducing the risk to the organization by positioning the risky interaction as far away as possible from the central players.

5.2 Approximating Optimal Heterogeneous Covert Networks

In section 5.1 it was established that if there exists exactly one pair of individuals that conduct an interaction that presents a high risk to the organization they should have the least connection to the remainder of the network (theorem 5.1). In this section we are interested in *which* connected graph $g \in \mathbb{G}^n$ should be adopted given the fact that the pair of individuals $i, j \in V$ conducting the risky interaction is the one that minimizes $d_i + d_j$. We approximate the graphs that are optimal in this respect by simulation.

We conducted a greedy optimization algorithm as follows.

Algorithm for approximating optimal single risk interaction network.

```
Input:
Initial graph $g^n_{initial}$.
Value of risky interaction $z$.
Number of times edges are added $m$.
Initialization:
$\bar{g} = g_{initial}$. (Denote $\bar{g} = (V, E)$).
$\mu(g_{help}) = 0$.

Iteration 1:
For i = 1:m

    Iteration 2:
    For $kl \in E^c$
        Step 1. Set $g' = \bar{g} \cup kl$.
        Step 2. Determine $i, j \in g'$ such that $d_i + d_j$ is minimal and locate $z$ at this link.
        Step 3. Compute $\mu(g')$.
        Step 4. If $\mu(g') > \mu(g_{help})$ set $g_{help} = g'$.

    End iteration 2.
    $\bar{g} = g_{help}$.

End iteration 1.
Output:
$\bar{g}$.
$\mu(\bar{g})$.
```

The best results of this greedy optimization are presented in table 1 for graphs of order $4 \leq n \leq 10$. The location of the pair of individuals that conduct the interaction that presents a high risk to the organization is presented in bold.

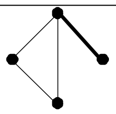
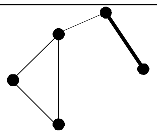
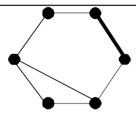
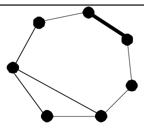
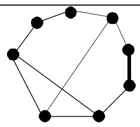
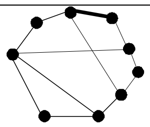
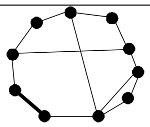
n	initial	final	μ
4	path		0.2813
5	path		0.2837
6	ring		0.3021
7	ring		0.3010
8	ring		0.3062
9	ring		0.3141
10	ring		0.3129

Table 1: Approximate optimal graphs with single high risk interaction, $z = 2$, indicated in **bold**.

As a further illustration optimal graphs of larger order are approximated by using the greedy optimization algorithm, see figure 7. It can be seen that cellular structures emerge around a centralized individual. Comparing these to figure 3 it can be seen that the networks in figure 7 are less dense. In addition it can be seen that the individuals conducting the interaction that presents the highest risk to the organization are members of a cell with limited connectivity to the remainder of the network.

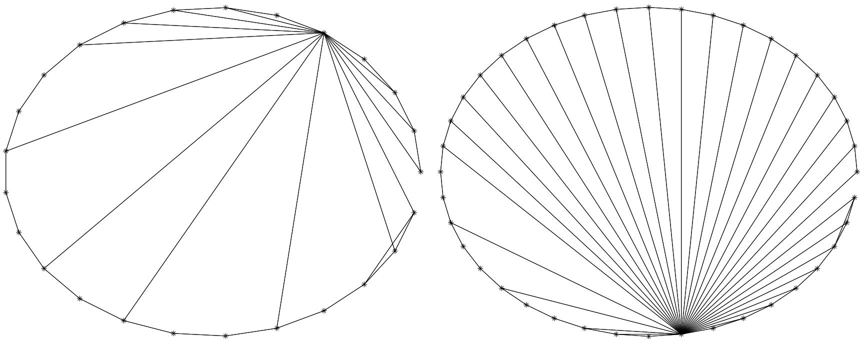


Figure 7: Approximate optimal graphs for n=25 (left) and n=40 (right).

References:

[1] Abuza, Z.(2003). Militant Islam in Southeast Asia. *Lynne Rienner Publishers: London.*

[2] Bergen, P.(2006). The Osama Bin Laden I Know: an Oral History of al Qaeda's Leader. *Free Press: New York.*

[3] Bollobas, B.(1998). Modern Graph Theory. *Springer-Verlag: New York.*

[4] Cammaert, A.P.M.(1994). Het Verborgen Front. *EISMA B.V.: Leeuwarden.*

[6] Cruickshank et al. (2007). Abu Musab Al Suri: Architect of the New Al Qaeda. *Studies in Conflict and Terrorism* Vol 30(1): 1-14.

[7] Engelen, D. (2005). De Nederlandse stay behind-organisatie in de koude oorlog, 1945-1992. *PIVOT-rapport nr. 166: 's Gravenhage.*

[8] Gunaratna, R. (2003). Inside Al Qaeda: Global Network of Terror. *Berkley Trade.*

[9] 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.*

[10] Johnson, L.K. (ed.)(2007). Strategic Intelligence: Covert Action–Beyond The Veils of Secret Foreign Policy, Vol 3. *Praeger Security International: Westport.*

[11] Koschade, S(2002). Indonesia Backgrounder: How the Jemaah Islamiyah Terrorist Network Operates. *International Crisis Group.*

[12] Koschade, S(2005). A Social Network Analysis of Aum Shinrikyo: Understanding Terrorism in Australia. *Proceedings Social Change in the 21st Century Conference, QUT Carseldine, Brisbane.*

[13] Koschade, S.(2006). A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence. *Terrorism and Political Violence* 29: 559-575.

[14] Lindelauf, R.H.A., Borm, P. and Hamers, H. (2008). The Influence of Secrecy on the Communication Structure of Covert Networks. *CentER Discussion Paper, 2008-23*, pp. 1-18.

[15] 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.

[16] Petraeus, D.H. et al.(2007). The U.S. Army Marine Corps Counterinsurgency Field Manual. *University of Chicago Press: Chicago.*

[18] Sageman, M.(2004). Understanding Terror Networks. *University of Pennsylvania Press: Philadelphia, Pennsylvania.*

[19] Vidino, L.(2006). Al Qaeda in Europe: The New Battleground of International Jihad. *Prometheus Books: New York.*

[20] Weiner, T(2007). Legacy of Ashes: The History of the CIA. *Doubleday.*